Deberes y responsabilidades de los servidores de acceso y alojamiento

Iglesias Portela, Maria José

Published in:
Deberes y responsabilidades de los servidores de acceso y alojamiento : un análisis multidisciplinar

Publication date:
2005

Document Version
le PDF de l'éditeur

CAPÍTULO XI

DEBERES Y RESPONSABILIDADES DE LAS UNIVERSIDADES PÚBLICAS A LA LUZ DE LA LSSICE. EN ESPECIAL LA ACTIVIDAD DE INTERMEDIACIÓN

MARÍA JOSÉ IGLESIAS PORTELA

1. INTRODUCCIÓN

El artículo que se presenta a continuación constituye un trabajo en desarrollo [1]. Su fin es determinar el régimen jurídico de la Universidad Pública como prestadora de servicios de intermediación y, especialmente, la búsqueda de herramientas que legitimen algunos de los controles que las universidades realizan sobre la red y alivien su responsabilidad por los daños causados por los destinatarios de los servicios prestados.

Se definirán en primer lugar el tipo de servicios que generalmente prestan las universidades, las infraestructuras y los mecanismos básicos para su prestación (2). Posteriormente se analizarán las obligaciones específicas impuestas por la LSSICE: los deberes de información y el deber de retención de datos, que nos darán pie a estudiar otros deberes relativos a la protección de datos, el secreto de las comunicaciones y la intimidad, todo ello en relación con los sistemas de vigilancia (3). En el apartado final trataré la responsabilidad de la Universidad por los daños que pudieran causar los destinatarios del servicio (4).

[1] El presente trabajo forma parte de la investigación que la autora está realizando en torno a la utilización de obras protegidas por los derechos de autor en la enseñanza en línea. Las conclusiones alcanzadas no son definitivas, por lo que cualquier crítica será sinceramente bienvenida (*maria.iglesias@uib.es*).

2. La Universidad Pública como Prestadora de Servicios de Intermediación

2.1. Servicios Prestados

La función de la Universidad es prestar el servicio público de la educación superior. Para ello lleva a cabo diferentes actividades, algunas de carácter obligatorio y otras complementario, al auxilio de las cuales, y de manera creciente en los últimos tiempos, pone a disposición de la comunidad universitaria determinados servicios de la sociedad de la información. Los destinatarios del servicio, por regla general, son los miembros de la comunidad universitaria, tanto sus centros o estructuras como las personas individuales pertenecientes a los tres estamentos básicos de la institución: personal docente e investigador (PDI), personal de la administración o servicios (PAS) y alumnos.

La actividad de intermediación se configura por lo tanto como un instrumento excepcional que se proporciona a los destinatarios para facilitar la consecución de sus objetivos [2]. Sin embargo no es una obligación *ex lege*, y por lo tanto su configuración y régimen jurídico dependerá de la voluntad de cada uno de los centros, siempre sujeta a la Constitución y el resto del ordenamiento jurídico. El punto de partida para especificar los deberes y responsabilidades de las universidades es la pregunta sobre el tipo de servicios que prestan, que, efectivamente, son los servicios «típicos» de la sociedad de la información: intermediación y provisión de contenidos. Me limitaré al estudio de las principales actividades de intermediación, a saber: acceso a la red y alojamiento permanente. A continuación se ofrece una somera descripción de los servicios más comunes prestados por las instituciones educativas [3]:

— *Acceso a Internet y transmisión de datos.* Las universidades públicas tienen su propia red local, su Intranet, que se conecta al exterior a través de la infraestructura proporcionada por RedIRIS, posibilitando así la conexión a la Red y la transmisión de datos desde diversos terminales que se conectan al servidor/es de la universidad. Los ordenadores suelen estar permanentemente conectados a la red y las IPs asignadas son en la mayoría de los casos IPs estáticas. La conexión puede ser local, cuando se realiza desde terminales propios del centro, o remota, mediante aplicaciones que permiten a los destinatarios conectarse desde el exterior a la red de la institución. El acceso local implica la utilización de ordenadores de sobremesa de uso privado [4] —en el caso del PDI y PAS— o compartido —sin perjuicio de que para su utilización en algunos centros sea necesaria la previa inserción de una clave de acceso, manualmente o mediante tarjeta magnética, que facilita la identificación del usuario [5]—.

Para agilizar la transmisión, se ofrece el servicio de proxy/caché, consistente en el almacenamiento de datos en servidores cercanos a los destinatarios, ahorrando tiempo en la descarga de la información a la vez que se descongestionan las vías de comunicación.

— *Correo electrónico.* El correo electrónico es ya una herramienta de uso común en las universidades, aun cuando algunas limitan el servicio a miembros del PDI o del PAS. Las normas de utilización del correo electrónico en el ámbito de las universidades públicas españolas difieren en su ámbito estrictamente académico o personal [6].

[2] La prestación de servicios de la sociedad de la información sería una «actividad instrumental y estratégica», *vid.* B. Peña, «Sociedades Mercantiles y Civiles», en VV. AA. *IV Seminario sobre Aspectos Jurídicos de la Gestión Universitaria II,* Gerona, 2001, pág. 573. Puede incluso afirmarse que muchos de los servicios que las universidades ofrecen a sus destinatarios van más allá del servicio público de la educación superior, ofreciéndoles la posibilidad de adscribirlos a un uso privado de algún modo ajeno a la actividad educativa.

[3] Para una introducción a los aspectos técnicos de los diferentes servicios de intermediación, *vid.* en este volumen, M. Payeras, Los servidores de acceso y alojamiento: descripción técnica y legal, apdos. 3.2. (Servicios proporcionados por los intermediarios de acceso), 4.3. (Tipos de servicios de provisión de espacio de alojamiento) y 4.4. (Otras formas de alojamiento de información).

[4] Cabe la posibilidad de que el personal, especialmente el personal docente, se conecte a la red con ordenadores de su propiedad, en cuyo caso se complica la problemática general que suscita el registro y acceso a las dependencias de trabajo, (*vid.* infra 3.2.B.f).

[5] La utilización o puesta a disposición de los equipos informáticos no es propiamente un servicio de la sociedad de la información, aunque las normas que regulan su uso sí formarán parte del ordenamiento específico aplicable a los destinatarios de este tipo de servicios.

[6] Por regla general las universidades limitan el uso del correo electrónico a actividades estrictamente docentes, de investigación o de gestión; así la universidad de Granada (*vid.* Normativa de uso de los recursos informáticos y de comunicaciones de la Universidad de Granada en *http://www.ugr.es/~ofiinfo/Segurida.htm*) y la de León (*vid.* apdo 3.2 de las Normas de Utilización de los Recursos Informáticos, accesibles en *http://www.unileon.es/modelos/archivo/norregint/20030829074240RecursosinformaticosdelaUle.rtf*). Permiten con carácter incidental el uso personal, la Autónoma de Barcelona (*vid.* Termes i condicions d'ús del correu electrònic, accesibles en *http://si.uab.es/si/comunicacions/antispam.html*), la Autónoma de Madrid (*vid.* Normas de uso del servicio de correo electrónico, en *http://www.uam.es/servicios/ti/cau/doc/*), la Universidad de la Laguna (cfr. Condiciones de uso del servicio de correo electrónico, accesibles a través de *http://w3.ccti.ull.es/ccti/frames.asp*), la Universidad de Oviedo (Normas de uso del correo electrónico,

— *Listas de distribución.* Las universidades dan acceso a listas de distribución propias y a listas externas como las de RedIRIS. Algunas posibilitan la creación de nuevas listas aunque generalmente se limita a personal PDI o PAS. Cada lista tiene un administrador con privilegios de gestión. Pueden ser moderadas y no moderadas, y el grado de moderación es variable, siendo el más intenso el que requiere la aprobación por parte del administrador del contenido de los mensajes. Las listas pueden tener además servicios adicionales tales como un espacio ftp para el almacenamiento de archivos accesibles a todos los miembros de la lista.
— *Grupos de noticias.* El servicio de *news* o foros de noticias puede ser local, restringido a la propia universidad, o externo, generalmente de RedIRIS. En este último caso el protagonismo de las diferentes instituciones afiliadas varía en función de su capacidad de gestión, así mientras existen ciertos nodos primarios de almacenamiento a cargo de los centros con estructura suficiente, RedIRIS actúa como nodo terminal de aquellas entidades que no disponen de recursos para proveer este servicio.
— *FTP.* El acceso al servidor *ftp o* a los espacios de disco virtual puede estar limitado a determinados usuarios o ser anónimo, sin que se requiera identificación previa. Asimismo, dependiendo del tipo de usuario, el acceso puede estar limitado a la consulta o descarga de ficheros o incluir privilegios de escritura permitiendo la incorporación de archivos.
— *Hospedaje Web.* El servicio de almacenamiento de páginas web también suele limitarse a centros orgánicos de la universidad, por ejemplo el espacio designado a un departamento. En este supuesto estamos ante un servicio que supera el de la mera intermediación para situarse en el ámbito de la provisión de contenidos. Aún en estos casos, existe la posibilidad de que en las páginas de contenidos propios de la universidad se incorporen sin control previo contenidos de terceros, tal y como ocurre cuando su configuración responde a una estructura dinámica, en la que se permite que el destinatario potencial de la página inserte datos para su visualización (por ejemplo un tablón de anuncios), que nos remite

en *http://directo.uniovi.es/Documentacion/normas_correo.asp*) y la Universidad de Vigo (Condicións e términos de uso do correo electrónico, en *http://www.seinv.uvigo.es/normativa/sistemas/condicionscorreo.htm*). Pese al tenor de las normas, entiendo que existe un uso tolerado del correo (más allá del incidental) como de los restantes recursos informáticos en todas las universidades.

nuevamente a la normativa sobre intermediarios. Todo ello sin perjuicio, y aquí sí nos movemos estrictamente en el ámbito de la intermediación, de los centros que autorizan la creación de páginas personales o pertenecientes a organizaciones desvinculadas de la estructura orgánica de la universidad, en los que ésta, pese a las apariencias, actúa como mero intermediario [7].

2.2. La regulación interna de los servicios de la sociedad de la información

Hoy por hoy la mayoría de los centros han regulado, con carácter más o menos intenso y más o menos reglado, la prestación de los servicios de intermediación a través de diferentes tipos de normas o políticas de uso [8]. La exigencia de reglamentación viene determinada y condicionada por la relación con RedIRIS y, especialmente, por los principios de seguridad jurídica y legalidad administrativa, que compelen a la delimitación de normas claras que especifiquen las condiciones de prestación de los servicios [9], de modo que —al igual que se re-

[7] Permiten el alojamiento de páginas personales entre otras: la Universidad de Valencia, la Autónoma de Madrid, la de Oviedo y la Autónoma de Barcelona. Para eludir posibles responsabilidades las universidades establecen normas que diferencian claramente entre las páginas de carácter institucional y las que no lo son.

[8] La configuración de la normativa de uso de los recursos informáticos diverge mucho en su naturaleza y extensión de unos centro a otros, así, mientras algunos han optado por un reglamento en el que se especifican de manera sistemática los deberes y derechos de los usuarios, otros han preferido establecer normas de uso individualizadas para el tipo de servicios, carentes, al menos aparentemente, de una estructura formal típica. Entre las primeras: Normas de uso del servicio de correo electrónico y Normas de uso aceptable y seguridad de la red de datos de la Universidad Autónoma de Madrid, aprobadas por el Consejo de Gobierno de 30 de abril de 2004; Normas y Recomendaciones de Uso de los Servicios de Informática de la Universidad Complutense de Madrid, aprobadas por el Consejo de Gobierno el 30 de enero de 2003; Normas de utilización de los recursos informáticos de la Universidad de León adoptadas por Acuerdo del Consejo de Gobierno de 12 de diciembre de 2002. Entre las segundas, la normativa de la Universidad de Cádiz, la de la Laguna, o más estructurada pero carente de unidad, la de la Universidad de Vigo.

[9] M. GÓMEZ, en *La Inactividad de la Administración*, Aranzadi, 2.ª ed. Aranzadi, 2000, págs. 339 et. seq., se refiere al «deber (de las Corporaciones Locales) de dictar el correspondiente reglamento regulador del servicio, cuando sea necesario para su establecimiento». Entiendo que las razones esgrimidas por el autor, resultan perfectamente aplicables al supuesto de la Universidad, en la medida en que los servicios de intermediación se dirigen «a unos potenciales usuarios, voluntarios u obligados, sobre cuya esfera de interés inciden, mejorándola o agravándola».

gula el servicio de préstamo en las bibliotecas—, se establezcan disposiciones que definan cada servicio prestado y sus características, las categorías de usuarios a los que van dirigidos y sus derechos y obligaciones, con especial referencia a la protección de datos personales, a los procedimientos para la suspensión del servicio, y, si fuere relevante, al régimen disciplinario. La delimitación de unas normas claras y precisas prevendrá no pocos conflictos que hoy en día tienen ya lugar en el ámbito universitario [10], no olvidemos que la falta de una regulación clara y específica jugará a favor de los usuarios. Ello promoverá además el conocimiento por los destinatarios del servicio del alcance de sus acciones y de la responsabilidad en la que pueden incurrir. De hecho, en el derecho comparado se le ha venido exigiendo a la instituciones docentes una suerte de diligencia *in educando* [11].

[10] Así lo advierte en su EdM la normativa de la Universidad de Valencia, refiriéndose explícitamente a la actividad no institucional. Los incidentes habidos en las universidades españolas son considerables. *Vid.* OTEMÍN, C. (moderador) Sesión IX-Mesa redonda: Conciliando derechos y obligaciones en la Red, *Jornadas Técnicas RedIRIS 2003*, Palma de Mallorca, se puede acceder a una reproducción de la sesión, formato vídeo windows media, en *http://www.rediris.es/jt/jt2003/archivo-jt*, o D. MARÍN, «La responsabilidad en el uso de los recursos informáticos», en *Revista de la Universidad Carlos III*, marzo 2000, núm 11, en *http://www.uc3m.es/uc3m/revista/num11.pdf*. También ha advertido públicamente de los peligros que supone en uso inadecuado de la red la Universidad del País Vasco en su comunicado «Medidas urgentes ante los últimos problemas de red», en *http://www.ehu.es/si/*, que alude a los «equipos ... que utilizan programas de intercambio de archivos, conocidos como *peer-to-peer*, utilizados principalmente para descargar música, videos y software ilegal».

[11] *Vid.* sección 110 (2)D(i) *Copyright Act*, relativa a la excepción educativa para la enseñanza a distancia que exige para su disfrute que la institución que utilice materiales protegidos por la propiedad intelectual «(i) institutes policies regarding copyright, provides informational materials to faculty, students, and relevant staff members that accurately describe, and promote compliance with, the laws of the United States relating to copyright, and provides notice to students that materials used in connection with the course may be subject to copyright protection». O, en general, respecto de la exención de responsabilidad por la actividad de provisión de alojamiento de las instituciones educativas la sección §§512 (e)1C *Copyright Act*: «Limitation on Liability of Nonprofit Educational Institutions. —(1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if—.

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended,

Los acuerdos que cada una de las universidades tiene con RedIRIS requieren la transposición de algunas de las responsabilidades asumidas al ordenamiento interno del centro. Según diferentes versiones del borrador de Acuerdo de Intención [12] las instituciones afiliadas se comprometen a cumplir con la Política de Uso de RedIRIS e informar de ella a los usuarios, además de a elaborar sus propias políticas de uso [13].

Los acuerdos de afiliación comportan determinadas obligaciones para la institución afiliada cuyo incumplimiento puede acarrear la suspensión del servicio o su retirada indefinida. Respecto de los usuarios se indica que deberán utilizar eficientemente la red, considerando inaceptables aquellas actividades que persigan o tengan como consecuencia: (1) la creación o transmisión de material que perjudique la dinámica habitual de los usuarios de RedIRIS, (2) la congestión de los enlaces de comunicaciones o sistemas informáticos, (3) la destrucción o modificación premeditada de la información de otros usuarios, (4) la violación de la privacidad e intimidad de otros usuarios o (5) el deterioro del trabajo de otros usuarios. Se reitera además que los usuarios, bajo ningún concepto, deberán usar los servicios de RedIRIS para fines privados o personales, fines lúdicos o fines comerciales, ajenos a las actividades propias de la institución. Finalmente se resuelve que las universidades son las responsables ante la RedIRIS del comportamiento de sus usuarios [14] y se les asigna el deber de velar por la legalidad en el uso del sistema.

within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than 2 notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright».

[12] El Acuerdo de Intención es el «contrato» existente entre RedIRIS y la Institución afiliada, para más información sobre el procedimiento de afiliación se puede consultar *http://www.rediris.es/rediris/afiliacion.es.html*. Lamentablemente no he podido consultar el modelo vigente.

[13] *Vid.* Política de Uso de RedIRIS, borrador (2.3) de 11 de julio de 2002, accesible en *http://www.rediris.es/rediris/aup.es.html*, apartado 3. O, en relación con el deber de información a los usuarios de los objetivos de RedIRIS y los términos y condiciones de uso, el apartado 5 del Anexo I (Política de Afiliación a RedIRIS), del Borrador de Solicitud de Afiliación a RedIRIS, en *http://www.rediris.es/rediris/PERs/RedIRISafiliacion.pdf*.

[14] Algunas universidades han incluido en sus normas de uso disposiciones en las que claramente atribuyen al usuario toda la responsabilidad por el uso que realice del sistema y expresa-

Atendiendo a la relevancia de las obligaciones transcritas, los centros deberán incorporar estas disposiciones a su propio ordenamiento, bien mediante la simple publicación de las políticas existentes —complementadas en su caso por disposiciones de desarrollo—, bien mediante su incorporación en la normativa interna reguladora de los recursos informáticos.

3. La LSSICE

3.1. Aplicabilidad de la LSSICE a las actividades de intermediación de las Universidades Públicas

El objetivo de este artículo es determinar el régimen jurídico de la prestación de servicios de intermediación por parte de las universidades. Tal régimen jurídico pretende ser el derivado, con las peculiaridades que la naturaleza de los protagonistas exija, de las disposiciones de la LSSICE, por lo que resulta necesario analizar la aplicabilidad de la norma al conjunto de las actividades mencionadas.

La ley regula «el régimen jurídico de los servicios de la sociedad de la información» y en especial, «las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios». Pese a que a primera vista pudiera resultar una obviedad, cabe preguntarse si la finalidad de la ley es regular el

mente se exoneran de cualquier responsabilidad al respecto, (así la Universidad de Oviedo, la de Vigo y la Autónoma de Madrid). El valor de dicha cláusula es relativo. El régimen de responsabilidad dependerá del contexto en el que se lleve a cabo el uso concreto, la declaración unilateral de la universidad no es presupuesto suficiente para derogarlo. El efecto de las cláusulas de exoneración de la responsabilidad es más bien intimidatorio. En este sentido *vid.* G. Sutter, *FE/HE Institutions and Liability for Third Party Provided Content,* pág. 11, en *http://www.jisc.ac.uk/uploaded_documents/GS_Content_Regulation.pdf.* En palabras del autor «It may be desirable to include in the AUP (acceptable use policies) some form of limitation of liability clause whereby the user agrees to indemnify the institution against any liability incurred as a result of the actions of that individual. This will not prevent the institution from incurring liability in the courts. However, should this happen it will, assuming the clause is not "unfair" under the terms of, for example, the Unfair Contract Terms legislation, entitle the institution to sue the user for recovery of any damages paid out. While in practical terms an individual student or academic is highly unlikely to have the economic resources to meet such a claim, this may help to impress upon users the importance of adhering to the rules regarding the use of institutional internet facilities».

régimen jurídico de *todos* los servicios de la sociedad de la información, independientemente de quien los preste (el sector privado o la Administración) o de la naturaleza del servicio [15]. Rememoremos el concepto de servicios de la sociedad de la información de la LSSICE, definido en el Anexo de la norma como «todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios».

La clave está entonces en determinar si determinados servicios prestados por la Administración, en nuestro caso, el servicio de enseñanza y, en especial, los servicios adicionales o instrumentales prestados en el marco de la actividad de las universidades, constituyen una actividad económica. La Ley 39/1988 de las Haciendas Locales, en su Tit. II, Cap. II, subsección 3.ª relativa al Impuesto de Actividades Económicas, al definir el hecho imponible del impuesto entiende que son actividades económicas el «ejercicio en territorio nacional, de actividades empresariales, profesionales o artísticas», (art. 79), considerando que «una actividad se ejerce con carácter empresarial, profesional o artístico, cuando suponga la ordenación por cuenta propia de medios de producción y de recursos humanos o de uno de ambos, con la finalidad de intervenir en la producción o distribución de bienes o servicios» (art. 80). Esta afirmación es suficiente para entender que, efectivamente, cuando una universidad presta servicios de intermediación a la comunidad universitaria realmente está ordenando por cuenta propia (independientemente del origen de los fondos) medios de producción y recursos humanos, con la finalidad de intervenir en la producción o distribución de servicios, opinión que corrobora el art. 83.1 apartados a) y b); por lo que, en definitiva, cabe concluir que los servicios de intermediación prestados por los centros educativos son servicios de la sociedad de la información a efectos de la LSSICE.

Distinto es el resultado al analizar la aplicabilidad de la Directiva 2000/31, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DCE) pongamos por caso, para el supuesto de una errónea implementación por parte de un estado, y la argumentación de su efecto directo. Al referirse al concepto de servicios de la sociedad de la información, la Directiva, se remite, (conside-

[15] La opción por la aplicabilidad de la LSSICE a la Administración Pública ha sido defendida por J. Valero en el Capítulo VI, apdo. 3 de esta obra.

rando 17) a la Directiva 98/34, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas, a su vez modificada por la Directiva 98/48. Según el considerando 19 de la Directiva 98/34, «por servicios se ha de entender, con arreglo al artículo 60 (hoy 50) del Tratado, tal como ha sido interpretado por la jurisprudencia del Tribunal de Justicia, las prestaciones realizadas normalmente a cambio de una remuneración; que esta característica no se da en las actividades que realiza el Estado, sin contrapartida económica, en el cumplimiento de su misión, principalmente en los ámbitos social, cultural, educativo y judicial; que, por ello, la definición del artículo 60 del Tratado no abarca las normas nacionales relativas a estas actividades y que, por tanto, dichas actividades no entran en el ámbito de aplicación de la presente Directiva».

A la luz del texto y de las remisiones de la Directiva 2000/31, puede interpretarse que la actividad administrativa en nuestro ámbito de estudio no cae en su ámbito de aplicación. Sin embargo, y retomando la norma española, son necesarias algunas observaciones. En primer lugar, el ámbito de aplicación de la DCE no ha de ser, ni en efecto es, el ámbito de la ley española. La norma europea tiene como finalidad garantizar la libre prestación de servicios (aun cuando sus efectos tengan otras implicaciones) por medio de una armonización normativa de mínimos. El *quid* estaría por lo tanto en determinar si la ley española acomete estrictamente la transposición de la DCE o, además, aspira a establecer el régimen jurídico específico de todos los servicios de la sociedad de la información (con independencia de que éste coincida *cuasi* literalmente con el contenido material de aquella). Entiendo que el propósito de la LSSICE es establecer el régimen jurídico de todos los servicios de la información no sólo por imposición europea, sino porque es un objetivo deseable si en verdad pretende otorgarse una mayor seguridad jurídica, tanto para los operadores como para los destinatarios de los servicios (*vid.* EdM LSSICE). Siempre que resulte posible y no del todo incompatible con la naturaleza de servicio público, hemos de movernos en este ámbito. Pero además, y aún pese a la remisión del legislador europeo, ha de tenerse en cuenta el contexto normativo en el que se desarrolla el concepto reflejado en la Directiva 98/48. Su objeto es establecer un sistema de comunicación de la actividad del legislador nacional a efecto de facilitar el principio de libre circulación, de manera que se eviten las legislaciones sectoriales que pudieran afectar negativamente a una de las cuatro libertades básicas del Tratado, pero desde la posición del que presta el servicio, sin perjuicio de que ello juegue en beneficio de los destinatarios de los bienes o servicios. A diferencia de otras normas comunitarias no tiene la Directiva 98/48 un objetivo garantista para los consumidores o los destinatarios. En lo que no atañe a este

ámbito concreto, y quedan fuera del mismo las actividades que los Estados lleven a cabo sin contrapartida económica en el cumplimiento de su misión educativa, no le interesan al legislador europeo las resoluciones adoptadas por cada uno de los estados, al afectar poco o nada a las cuatro libertades, por lo que no le impone la obligación de comunicarlas. El concepto del considerando 19 ha de quedar por lo tanto limitado a este contexto y no ha de trasladarse necesariamente al concepto que adopten las normas estatales.

Es verdad que hay otras razones y fundamentos válidos para argumentar que la LSSICE no se aplica en general a la Administración y en especial a las actividades educativas [16], pero teniendo en cuenta que la no aplicación de la LSSICE podría conducir desde una perspectiva material a situaciones contrarias al sentido común [17], y considerando que en última instancia éste ha de ser de facto el principio inspirador de todo ordenamiento, abogo, de conformidad con las razones expuestas, por su aplicación. Así parecen entenderlo algunas universidades españolas que hacen referencia explícita a la LSSICE [18] como norma aplicable a los servicios que prestan.

[16] Del texto de la LSSICE puede concluirse que el legislador no tenía en mente la prestación de servicios por las Administraciones Públicas al emprender la tarea de regular los servicios de la sociedad de la información. Pese a que no se hace ninguna exclusión explícita de la Administración, sí se establecen algunas disposiciones que pudieran resultar extrañas (las relativas a la responsabilidad) o inadecuadas (por ejemplo las referentes a la contratación, término en el que no parece tener cabida el perfeccionamiento del contenido obligacional de la relación de prestación con los administrados) a la actividad administrativa. De hecho, sólo hay una disposición que claramente hace referencia a la Administración como prestadora de servicios de la sociedad de la información: la Disposición Adicional Quinta, relativa a la accesibilidad. El silencio del legislador se revela al esgrimir los títulos competenciales de la ley, entre los que se echa en falta cualquier referencia al artículo 149.18.1.ª de la Constitución. Por otro lado, bien es cierto que puede acudirse a otros instrumentos del ordenamiento para hallar, exceptuando tal vez el tema de la mal llamada contratación electrónica y no sin esfuerzos interpretativos, soluciones similares a la alcanzada por el legislador.

[17] R. MARTÍNEZ, *Informe sobre la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y Comercio Electrónico*, Documento Interno de la Universidad de Valencia. También J. VALERO, en este mismo volumen (Capítulo VI, apdo. 3), ha insistido en las diferentes razones que justifican la aplicación de la LSSICE a las Administraciones Públicas.

[18] Por ejemplo, la Universidad de Málaga, la de Alicante o la de Vigo. También en el ámbito europeo se viene reconociendo la aplicación de las normas de implementación de la Directiva de comercio electrónico a las instituciones educativas que ofrecen servicios de intermediación; en relación con el Reino Unido, cfr. G. SUTTER, *op. cit.* nota 14.

3.2. Los deberes de la LSSICE

A. *Deberes de información*

Los deberes de información otorgan a los destinatarios del servicio (y a los organismos públicos encargados de su supervisión) cierta confianza sobre la identidad del prestador y el contenido de los servicios prestados [19]. La LSSICE se ocupa, en su artículo 10, de la información sobre el prestador, sin mención directa a los datos relativos al contenido del servicio (salvo, y resultando cuanto menos asistemático y extraño a la coherencia del precepto, el apartado relativo al precio del producto o servicio). A falta de disposiciones específicas se ha de acudir a otras normas del ordenamiento relativas al contenido o funcionamiento del servicio, cuyo espíritu y principios informadores, se erigen en instrumento de garantía para el destinatario de los servicios estudiados; entre ellas, la Ley General para la Defensa de los Consumidores y Usuarios [20], la Ley Orgánica de Protección de Datos de Carácter Personal o, en los extremos en los que resulte aplicable, la Ley General de Telecomunicaciones, de ahora en adelante LGT.

a) *Deberes relativos al prestador de servicios* [21]

De conformidad con el artículo 10 de la LSSICE, las universidades que presten servicios de la sociedad de la información, deberán poner a disposición del destinatario del servicio (la comunidad universitaria, y, en su caso, los ciudadanos en general) información relativa a «su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva» (art. 10.1.a) y su número de identificación fiscal (art. 10.1.e). No plantean estos preceptos problema alguno, aunque en la práctica son escasas las universidades que los implementan en toda su extensión.

Especial consideración merece la letra c) en tanto exige, para los supuestos en los que la actividad en concreto estuviese sujeta a una autorización, que se proporcionen los datos relativos a la autorización y los identificativos del órgano competente encargado de su supervisión. En nuestro ámbito, y para todas las actividades consideradas como servicios de la sociedad de la información, basta la referencia a la norma de creación y reconocimiento de la universidad por el poder legislativo de la Comunidad Autónoma o de las Cortes Generales. Más problemas plantea la pertinencia de cumplir o no con los requisitos relativos a la identificación del órgano competente de su supervisión, por un lado por el complejo sistema de organización (y autoorganización) de las universidades, ya que, dependiendo del sector del que se trate, la supervisión del funcionamiento dependerá de un órgano u otro. Con carácter general, puede hacerse referencia al órgano de la Comunidad Autónoma o de la Administración de Estado con competencias en educación superior. Sí considero conveniente la mención expresa a la autoridad encargada de la supervisión o control de los servicios de intermediación.

Aunque tengo mis dudas, podría exigírsele a aquellas universidades que presten servicios que caigan en el ámbito de aplicación de la Ley General de Telecomunicaciones, la referencia a la notificación de la Comisión del Mercado de Telecomunicaciones de inicio de actividad o, en su caso, a las autorizaciones obtenidas a tal efecto de conformidad con la antigua ley [22]. En todo caso, se deberá comunicar al menos su nombre de dominio o dirección de Internet (art. 9.1 LSSICE) al Registro de operadores creado en virtud del artículo 7 de la LGT.

[19] Los deberes de información de la LSSICE han sido analizados en el Capítulo II de este volumen por S. CAVANILLAS, a quien me remito para suplir la información de este apartado.

[20] El proyecto de Solicitud de Afiliación a la RedIRIS parece someter la prestación de los servicios a la normativa de consumidores, en tanto dispone en su anexo II, apartado 1 que «Las instituciones afiliadas velarán especialmente para proteger... e) al consumidor: para respetar los principios de transparencia y accesibilidad, sometiéndose a las normativas de protección del consumidor».

[21] Sólo haré referencia a los apartados del artículo 10 que han de observar las universidades como prestadoras de servicios de intermediación. La letra d) se refiere a la información que deberán proporcionar aquellos que ejerzan una profesión regulada. Profesión regulada es «la actividad o conjunto de actividades profesionales para cuyo acceso, ejercicio o alguna de sus modalidades de ejercicio se exija directa o indirectamente un título y constituyan una profesión en un Estado miembro», entre las que se incluye la del profesor de universidad, (art. 1 en relación con el anexo 1 del Real Decreto 1665/1991). En principio, no puede afirmarse la aplicabilidad de la letra d), con carácter general, a las universidades (aún siendo más discutible si ello sería aplicable por ejemplo a las páginas web de los cursos de los profesores). Pese a ello, y pecando en un exceso de analogía, sí considero oportuno, en aras a la transparencia, que se proporcione información relativa a sus principales normas reguladoras y los medios través de los cuales se pueden conocer, incluidos los electrónicos (apartado 4 de la letra d), tal y como por otro lado vienen haciendo por regla general las universidades españolas en su página web.

[22] Son titulares de una autorización tipo C la Universidad de Murcia (Resolución de la Comisión General de Telecomunicaciones de fecha 29 de enero de 2003), la Universidad de Zaragoza (Resolución de la C.M.T. de 20 de diciembre de 2001), y la UPCnet de la Universidad Politécnica de Cataluña, (Resolución de 27 de enero de 2000).

La letra g) del art. 10.1 impone a la universidad la obligación de informar sobre los códigos de conducta [23] a los que esté adherida y la manera de consultarlos electrónicamente. Si ésta elabora su propio Código, deberá promover la participación de los usuarios, que podemos considerar queda del todo garantizada si lo aprueba o interviene en su elaboración alguno de los órganos en los que se dé la representación de toda la comunidad universitaria, por ejemplo, el Consejo de Gobierno.

b) *De los servicios prestados*

La LSSICE no impone ninguna obligación de información relativa a los servicios prestados. En los acuerdos de afiliación, la RedIRIS determina algunas indicaciones que deberán darse a los usuarios, que más que relativas a sus derechos, se relacionan con sus deberes y tienen generalmente como fundamento la seguridad y el buen y racional uso del servicio [24]. Más allá de las obligaciones derivadas de los acuerdos de afiliación, las universidades deberán informar a los destinatarios de los derechos y deberes que implica el disfrute del servicio, sin perjuicio de las obligaciones específicas derivadas de la normativa de protección de datos [25]. La utilización de los recursos informáticos presupone al fin y al cabo la existencia de una específica relación obligacional cuyos extremos deberán conocer las partes a ella vinculadas. Los mecanismos utilizados al efecto han de ser lo más transparentes posible, proveyendo el acceso a la información de modo fácil y asequible, —por ejemplo mediante la publicación de las normas en las páginas web de la universidad y en las aulas de informática—. En todo caso, antes de completar el formulario de registro para la solicitud de un servicio, debe asegurarse el conocimiento o el acceso por los potenciales usuarios a las normas reguladoras, de manera que pueda concluirse el conocimiento de las condiciones y responsabilidades que supone el acceso a la red o el disfrute de una cuenta en el sistema. Finalmente cabe observar la tendencia en derecho comparado de incluir deberes de información de diversa naturaleza, para

[23] El concepto de código de conducta es un concepto indefinido en el caben diferentes manifestaciones de lo que se ha venido denominado autorregulación. Puede entenderse como código de conducta las normas de Abuso de Correo Electrónico de la RedIRIS que han suscrito y adoptado las universidades.

[24] *Vid.* supra 2.2.

[25] *Vid.* infra 3.2.B.

disfrutar de las exenciones de responsabilidad, so pena de incurrir en una falta de diligencia por culpa *«in educando»* [26].

B. ***El deber de retención de datos de tráfico y otros deberes relacionados con la protección de datos, el secreto de las comunicaciones y la intimidad***

El artículo 12 de la LSSICE establece la obligación de retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses [27]. La remisión a desarrollo reglamentario, la indeterminación que acusa el artículo 12 y la posible conculcación de los derechos fundamentales tipificados en el artículo 18 de la Norma Suprema requieren postergar la aplicación de la obligación de retención hasta la aparición del reglamento que garantice su ejercicio de conformidad con el resto del ordenamiento [28].

A salvo de estas apreciaciones, los datos de tráfico y su tratamiento son una realidad que ha de tratarse desde una doble perspectiva. Por un lado la de la protección de datos de carácter personal, en tanto los proveedores de servicios de la sociedad de la información vienen registrando y almacenando los datos con una justificación distinta a la que requiere el artículo 12. Por otro, la del secreto de las comunicaciones, ya que los datos de tráfico están amparados por el artículo 18.3 [29], constituyendo además el presupuesto básico de los sistemas

[26] *Vid.* nota 11.

[27] El art. 12 LSSICE ha sido tratado en varios capítulos de esta obra *vid.* P. GRIMALT, Capítulo VIII y J. VALERO, Capítulo V. También S. CAVANILLAS se ha referido a la responsabilidad civil por incumplimiento a los dispuesto en el precepto (Capítulo III).

[28] La conveniencia de postergar la aplicación del art. 12 la manifestó el propio Ministerio de Ciencia y Tecnología en una carta remitida a la AECE, en la que indicaba que el deber de retención de datos no resultaría de aplicación hasta que se realizara el desarrollo reglamentario previsto en al artículo 12.4. Se puede acceder a la trascripción de la carta en *http://www.aece.org/noticias2.asp?noti=419*. Pese a tales declaraciones, si atendemos a la información contenida en el portal que el mismo Ministerio ha puesto en marcha sobre la LSSICE (*http://www.lssi.es*), no parece que se mantenga esta interpretación, en tanto se indica que los prestadores de servicios de la sociedad de la información «... deben retener algunos datos relacionados con las comunicaciones electrónicas, para que las autoridades competentes puedan utilizarlos cuando se esté investigando un delito cometido a través de Internet. El deber de retención de datos no abarca los datos de navegación de los usuarios o el contenido de los mensajes que se intercambien por vía electrónica».

[29] *Vid.* infra 3.2.B.

de vigilancia o monitorización. Se abre así un nuevo frente de estudio que abarca dos de los extremos del artículo 18 CE: de la mano del secreto a las comunicaciones nos acompaña el derecho a la intimidad.

a) *Datos de tráfico y protección de datos*

El concepto de datos de tráfico es un concepto genérico, un cajón desastre en el que hay cabida para casi todo tipo de información que se pueda concluir de una comunicación. No es objeto de este artículo profundizar en la cuestión. Baste por el momento hacer referencia a la definición dada por la Directiva 2002/58 relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, de datos de tráfico como «cualquier dato tratado a efectos de una comunicación a través de una red de comunicaciones electrónicas o a efectos de facturación de la línea» (art. 2). «Los datos de tráfico pueden referirse entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o del destinatario, a la red en la que se origina o concluye la transmisión, al principio, fin o duración de una conexión. También pueden referirse al formato en que la red conduce la comunicación» (considerando 15). Pese a que la enumeración es claramente abierta, nos da una pista del criterio a adoptar para diferenciar los datos de tráfico de los que no lo son, que radica en su «tratamiento» a efectos de la comunicación y no en su «conocimiento» en virtud de la comunicación.

En todo caso, y en el contexto de la normativa de comunicaciones electrónicas y de protección de datos personales, deben considerarse datos de tráfico, sólo aquellos que el proveedor de servicios necesita —necesariamente trata [30]—, para llevar a cabo su función técnica, datos que divergirán en función del tipo de proveedor y del tipo de servicio prestado. Así mientras para el proveedor de acceso a la red, distinto al transmisor de datos, puede no resultar relevante la IP de destino de una conexión, ésta es absolutamente necesaria para un *encaminador*, para quien presta servicios de proxy/caché o, por supuesto, para los prestadores de servicios de correo electrónico. Esta conceptualización dista mucho del concepto vulgar de datos de tráfico que generalmente va acompañado de información «extra» que se obtiene fácilmente en virtud de la comunicación. Al adoptar la universidad casi todos de los roles de intermediación resulta significativo el diferente tipo de datos que puede almacenar o registrar como consecuencia de los servicios que presta y los riesgos que para los derechos de los usuarios de la red puede suponer su tratamiento.

Tradicionalmente la regulación de los datos de tráfico se realiza desde la normativa de las telecomunicaciones, partiendo de la base de que son los operadores de telecomunicaciones los que, por sus funciones técnicas, acceden a ellos. El funcionamiento de Internet expande este ámbito subjetivo en el que aparecen otros actores con acceso a los datos de tráfico. La irrupción de nuevos agentes se ha puesto de manifiesto en las últimas reformas normativas, tanto en la Ley 32/2003 General de Telecomunicaciones, así para los encargados de la conectividad, como en la LSSICE, para todos los intermediarios. A continuación se describirá brevemente el tratamiento específico que la LGT otorga a los datos de tráfico y el que resulta aplicable por defecto, es decir, el de la Ley 15/1999 de Protección de Datos de Carácter Personal (LOPDCP).

b) *La normativa de servicios de comunicaciones electrónicas*

La conservación o el tratamiento de los datos de tráfico deberá realizarse de conformidad con lo dispuesto por la Ley General de Telecomunicaciones, el Reglamento aún vigente (Real Decreto 1736/1998), y, en su caso, la Directiva 2002/58. El ámbito de aplicación de dichas normas merece al menos dos observaciones. Por un lado regulan sólo la actividad de los prestadores de servicios de Internet dedicados a la provisión de acceso y transmisión de datos, siendo más discutible si se aplican igualmente al servicio de *caché*. Por otro, en el caso de la ley española [31], y en relación a los derechos [32] relativos al tratamiento de los datos de tráfico, el legislador de una forma algo sibilina ha limitado su apli-

[30] S. Louveaux y M.V. Pérez Asinari apuestan por una interpretación restrictiva del concepto de datos de tráfico en su artículo «New European Directive 2002/58 on the Processing of Personal Data and the Protection of privacy in the Electronic Communication Sector-Some Initial Remarks», *Computer and Telecommunications Law Review*, 2003, Issue 133, págs. 137 y ss.

[31] La directiva limita su ámbito de aplicación a las comunicaciones electrónicas disponibles al público en las redes públicas de comunicación (art. 3.4) mientras que la norma española afecta también a las redes privadas, excepto en algunas de sus disposiciones como el artículo 33 relativo al secreto de las comunicaciones o el artículo 38.3 en el que se hace referencia a los derechos de los abonados y los usuarios. Según la definición del anexo de la norma, se considera usuario «una persona física o jurídica que utiliza o solicita un servicio de comunicaciones electrónica disponible para el público».

[32] Es cuanto menos curioso que en la LGT se considere un «derecho» del usuario la anonimización o cancelación de los datos de tráfico mientras en la Directiva 2002/58 se trata como un «deber» del prestador.

cación a las redes que prestan servicios de comunicación al público en general, tal y como claramente hace en relación al deber de respeto al secreto de las comunicaciones (art. 33), excluyendo de su mandato las redes privadas. No obstante, según ha entendido el Grupo de Trabajo de Protección de Datos Personales, las normas podrían cobrar vigencia cuando se envíe información fuera de la propia red [33].

Tanto la LGT (art. 38.3) como la Directiva 2002/58 (art. 6) imponen la cancelación o *anonimización* de los datos de tráfico cuando ya no sean necesarios para la transmisión, es decir, una vez ésta haya finalizado en todos sus extremos, con excepción de los datos necesarios a efectos de facturación [34] y sin perjuicio, entiende nuestra LGT, de lo dispuesto por el artículo 12 LSSICE. Además, ambas normas reconocen la posibilidad de conservar los datos de tráfico para fines distintos de la facturación, tales como la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido, requiriendo para ello el consentimiento del afectado [35]. El tratamiento ha de limitarse a los datos y al tiempo necesario para realizar tales actividades. Por su parte los artículos 33 y 34 de la LGT determina que los prestadores de servicios deberán garantizar el respeto al secreto de las comunicaciones y a la protección de los datos de carácter personal conforme a la legislación vigente.

c) *La normativa de protección de datos personales*

Como se adelantó en su momento, los datos de tráfico son a menudo almacenados y registrados durante un período más o menos largo de duración por

[33] Grupo de trabajo de protección de datos del artículo 29, Documento de Trabajo. Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. Adoptado el 21 de noviembre de 2000. 5063/00/ES/FINAL WP 37, pág. 26. Accesible en *http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2000/wpdocs00_en.htm.*

[34] Como han señalado S. LOUVEAUX y M.V PÉREZ ASINARI, la conservación de datos a efectos de facturación es cada vez menos relevante, al menos cuando los usuarios utilizan líneas ADSL. *Vid. op. cit.* en nota 30, pág. 136.

[35] F. H. HERNÁNDEZ, en su estudio «La intervención de las comunicaciones electrónicas», (accesible previa introducción de contraseña en http://www.fiscalia.org), admite el conocimiento tácito del perjudicado cuando los de datos de tráfico se utilicen para fines distintos de la efectiva transmisión de la comunicación, *vid.* pág. 30 y ss. El autor siguiendo las declaraciones del Consejo de Europa y del Grupo del Art. 29 llega a la conclusión de que incluso los datos de navegación están «sometidos a las mismas garantías de confidencialidad y secreto de las comunicaciones que los propios contenidos» íd.

todo tipo de proveedores de servicios de intermediación [36]. Su almacenamiento se realiza en ficheros *log* [37] o de registro que pueden ser generados automáticamente por el proveedor de acceso a la red, por el propio servidor de alojamiento, en los ordenadores de la red interna o en los de los usuarios.

La información contenida en los archivos *log* puede ser de diferente naturaleza y extensión, pero, con carácter general, suele concernir, por una parte a las direcciones de las máquinas del emisor y del destinatario (direcciones IP), a la fecha y la hora de la conexión, a informaciones técnicas que caracterizan el tipo de uso (acceso al Web, mensajería, etc...) —es decir, información de la misma naturaleza que los datos de tráfico—, y, por otra, a la petición o el mensaje propiamente dicho. Además los ficheros pueden contener datos que no son estrictamente necesarios para la actividad de comunicación, tales como la versión del navegador, las aplicaciones informáticas que tiene instalado el programa, el idioma utilizado, o, en el caso del correo electrónico, información contenida en la cabecera del mensaje, como el asunto o el nombre y tipo de documentos adjuntos. Concepto clave para considerar estos ficheros como contenedores de datos personales es el de la IP. Existe hoy en día un consenso más o menos generalizado en la consideración, bajo ciertas condiciones, de la IP como dato personal [38], afirmación especialmente adecuada —al menos en los supuestos en los

[36] Los diferentes intervinientes en los procesos de comunicación electrónica y prestación de servicios de alojamiento suelen registrar de forma sistemática determinada información, así «aunque sólo sea por motivos de seguridad, los proveedores de acceso a Internet parecen registrar siempre en un fichero, de forma sistemática, la fecha, la hora, la duración, la IP y la cantidad de datos transmitidos en el transcurso de una sesión» (Grupo de trabajo sobre protección de datos del artículo 29, Documento de Trabajo, Privacidad en Internet... págs 13 y 45, cit. en nota 33); por su parte los proveedores de alojamiento crean «sistemáticamente por defecto un fichero de registro o un fichero histórico que puede contener todos o algunos de los datos que aparecen en la cabecera de la petición http, además de la dirección IP. El fichero de registro es una práctica estándar y todos los servidores lo crean»(id. págs. 13 y 46). En el caso de servicios de proxy caché se «puede mantener una lista pormenorizada de visitas a sitios web conectados a una dirección IP en un momento determinado» (id. pág. 46).

[37] Ya en 1998 el Consejo de Estado Francés, en su estudio «Internet et les réseaux numériques» advertía de los riesgos que los archivos log presentan para la vida privada de los usuarios de la red. El informe es accesible en *http://lesrapports.ladocumentationfrancaise.fr/BRP/984001519/0000.htm.*

[38] Lo ha confirmado la Agencia Española de Protección de Datos en su Informe 327/2003: Carácter de dato personal de la dirección IP. Sobre la consideración de los datos contenidos en los archivos log como datos personales *vid.* M.V. PÉREZ ASINARI, «Legal Constrains for the Protection of Privacy and Personal Data in Electronic Evidence Handing», en *International Review of Law Computers & Technology*, volumen 18, núm. 2, julio 2004.

que la universidad adopta el rol del proveedor de acceso— al ámbito universitario en el que suelen utilizarse IPs fijas para cada máquina, resultando sencilla sino automática la vinculación entre una dirección IP y el usuario. En lo que a los puestos multiusuario se refiere, generalmente se implementan mecanismos de identificación, tales como la introducción de contraseñas o tarjetas con carácter previo al inicio de cada sesión, que facilitan la asociación de los datos con una persona determinada [39].

La universidad que opte por mantener este tipo de ficheros, —es decir por no cancelar o *anonimizar* los datos de tráfico en su acepción amplia o estricta—, deberá publicar su existencia (art. 20 LOPDCP) y cumplir con los restantes requisitos exigidos por la LOPDCP. En primer lugar, deberá informar a los afectados de la existencia del fichero. Según lo previsto en el artículo 5 LOPDCP la información deberá ser expresa, precisa e inequívoca sobre cada uno de los extremos contemplados, es decir, respecto de la relación de datos que serán almacenados, y en especial, respecto de la finalidad de la recogida. La creación y el mantenimiento de los ficheros ha de responder a los principios informadores de la LOPDCP. El principio de finalidad implica que ésta ha de ser determinada, explícita y legítima. Los centros educativos pueden almacenar los datos de tráfico con diversos fines, entre los cuales se encuentra, y es el que presenta mayor interés, la supervisión de la red. Su estudio, dada la afectación a otros derechos como el de la intimidad y el secreto de las comunicaciones, se postergará al siguiente apartado. En todo caso, los datos almacenados deberán ser tan sólo aquellos estrictamente necesarios para cumplir con los fines declarados (principios de calidad, congruencia, racionalidad y compatibilidad); si en virtud del almacenamiento automático se registra otra información no estrictamente necesaria para los fines del fichero deberá ser discriminada y eliminada. Asimismo, los datos sólo serán conservados durante el tiempo exigido por la finalidad esgrimida, cuando el objetivo concreto para el que hayan sido recolectados se haya agotado, ha de cesarse en el tratamiento y por lo tanto proceder a su cancelación.

Ex artículo 6.2 LOPDCP no se requiere el consentimiento del afectado cuando los ficheros son conservados a efectos de control interno de la red, al

[39] Asimismo se vienen implementando ciertos mecanismos de control no sólo respecto de la identidad del usuario que en cada momento utiliza la máquina sino igualmente de las operaciones que realiza. Para un ejemplo de estos sistemas se puede consultar la ponencia pronunciada por J. A LORENZO, J. C. LÓPEZ, P. CERDÁN et al. «ACUO: Aplicación de Control de Usuarios y Ordenadores» en las Jornadas de RedIRIS, Salamanca 2002, accesible en *http://www.RedIRIS.es/RedIRIS/boletin/62-63/index.es.html*.

almacenarse los datos en el marco de una relación de prestación con la Administración y responder su tratamiento al cumplimiento de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, concretadas, en el entorno que nos ocupa, en el ejercicio de su potestad de control sobre el funcionamiento, seguridad y uso de la red de la que es titular (art. 6 LOPDCP).

La universidad deberá cumplir con los requisitos de seguridad impuestos por la normativa de protección de datos [40]. La determinación del nivel de seguridad de los ficheros dependerá del tipo de datos almacenados que variará según el contenido de los archivos *log*. Cuando éstos incluyan datos de los que se pudiera afirmar que son o revelan datos sensibles, no son incongruentes las voces garantistas que exigen la seguridad máxima. Por otro lado en la gestión del tratamiento es especialmente relevante el deber de secreto profesional (art. 10 LOPDCP) sobre el contenido de los datos, que prohíbe su revelación con fines distintos a los previstos en la creación del fichero [41].

d) *Otras actuaciones relacionadas con la protección de datos*

Además de la información albergada en los «archivos *log*», el responsable de los servicios de red de la universidad maneja otro tipo de información personal derivada de los servicios de intermediación, tal como la relativa a los datos de usuarios de las listas de distribución, las direcciones IP, asignación de correos electrónicos, etc... Información cuyo almacenamiento y tratamiento, —siempre que no se encuentre en fuentes accesibles al público—, de-

[40] En el año 2001 la Agencia de Protección de Datos estimó que la Universidad de Castilla la Mancha había infringido la normativa de seguridad al crear un fichero con datos de carácter personal y alojarlo en una página web que, aunque desconocida para la mayoría de los usuarios, era de acceso público. En su resolución (APD R/0048/2001), sólo se tiene en cuenta la normativa de seguridad, sin embargo es destacable que se habían infringido además no pocos preceptos de la LOPDCP.

[41] Ha de señalarse que son pocas las normas de las universidades que hacen referencia expresa a la normativa de datos personales o a los diferentes tratamientos de datos que realizan. Se destaca el Reglamento de los Servicios Informáticos del País Vasco, en cuyo artículo 16.2 dispone que «Los titulares, operadores y usuarios están obligados en todo momento a respetar y reservar la intimidad del resto de los usuarios. En concreto, los titulares y operadores no podrán utilizar ni difundir la información personal o confidencial obtenida voluntaria o involuntariamente a través de los procesos de mantenimiento, operación o uso de los servicios informáticos y/o de red. Asimismo, en todo caso queda expresamente prohibido la suplantación de usuario para la realización de cualquier actividad».

berá cumplir con lo prescrito por la normativa vigente, y ello pese a lo gravoso que pudiera resultar ser para el centro.

e) *La justificación del tratamiento: monitorización y controles sobre el uso de la red. Secreto de las comunicaciones y derecho a la intimidad de los miembros de la comunidad universitaria*

La protección de los datos de tráfico por el artículo 18.3 CE, ha sido sostenida, aun refiriéndose a los sistemas de telecomunicación tradicionales, por la jurisprudencia del Tribunal Europeo de Derechos Humanos [42] y por el Tribunal Constitucional [43], además de contemplarse explícitamente en la Directiva 2002/58 [44].

[42] *Vid. caso Malone,* sTEDH de 2 de agosto de 1984 (TEDH 1984\1).

[43] Entre otras sTC 70/2002 (RTC 2002\70) y sTC 123/2002 (RTC 2002\123). Las repercusiones del secreto de las comunicaciones en el régimen específico de los datos de tráfico han sido puestas de manifiesto en la Circular de la Fiscalía General del Estado 1/1999 (RCL 2000, 876). Sobre la naturaleza de los datos de tráfico puede consultarse el estudio llevado a cabo por el Fiscal del Tribunal Superior de Justicia de Andalucía F. J. HERNÁNDEZ, «La intervención de las comunicaciones electrónicas», cit. en nota 35.

[44] El art. 5 .1 de la Directiva 2002/58 dispone que «Los Estados miembros garantizarán, a través de la legislación nacional, *la confidencialidad de las comunicaciones*, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, *sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad*». A tenor del art. 15 «Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una *medida necesaria proporcionada y apropiada* en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, *o la prevención, investigación, descubrimiento y persecución de delitos* o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea».

Ello implica que los accesos y tratamientos de los datos de tráfico distintos a los legalmente establecidos, requerirán previo levantamiento del secreto, que, en principio y de conformidad con el artículo 18.3 de la CE, sólo puede venir dado por el consentimiento del interesado, o cuando concurran determinadas circunstancias, mediante autorización judicial, prohibiéndose el acceso, registro o difusión de los mismos con un fin distinto del necesario para llevar a cabo la comunicación [45].

Hemos visto, no obstante, que el tratamiento de los datos de tráfico no requerirá el consentimiento de los afectados cuando «se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias». ¿Quiere esto decir que cuando los datos sean utilizados a tal fin no se les aplican las garantías que otorga el artículo 18.3? Por supuesto que no. Cuando el acceso y tratamiento de datos se adecue al juicio de proporcionalidad al que posteriormente nos referiremos no resulta necesario el levantamiento del secreto del afectado. Sin embargo cualquier exceso derivado del tratamiento supondrá, además de la vulneración de la normativa de protección de datos, la violación del secreto de las comunicaciones. Así lo ha entendido el Tribunal Constitucional al observar que el régimen de la cesión de listados telefónicos a las Fuerzas y Cuerpos de Seguridad del Estado es el derivado del art. 18.3 CE (es decir, autorización judicial) y no el del artículo 11.2 de la LOPDCP [46].

[45] No obstante ha de tenerse en cuenta, como ha señalado el Tribunal Constitucional en su sentencia 123/2002 (RTC 2002\123), refiriéndose a los listados telefónicos que incorporan datos relativos al número de destino, momento de la comunicación y su duración, que el acceso y registro de esta clase de datos supone una injerencia de menor intensidad que las que se refieren al contenido de la comunicación. En palabras del Constitucional «Dichos datos configuran el proceso de comunicación en su vertiente externa y son confidenciales, es decir, reservados del conocimiento público y general, además de pertenecientes a la propia esfera privada de los comunicantes. El destino, el momento y la duración de una comunicación telefónica, o de una comunicación a la que se accede mediante las señales telefónicas, constituyen datos que configuran externamente un hecho que, además de carácter privado, puede asimismo poseer un carácter íntimo. Ahora bien, aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las «escuchas telefónicas», siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad». En contra, sTS de 22 de marzo de 1999 (RJ 1999\2947), que consideró que la obtención del listado de registro de llamadas telefónicas no afecta al secreto de la comunicaciones sino que forma parte del conjunto de datos personales regulados por la LOPDCP.

[46] Cfr. sTC 123/2002 (RJ 1999\2947), cit. en nota anterior.

Sentadas estas premisas hemos de preguntarnos por la instrumentalidad del tratamiento de los datos de tráfico, es decir, por su finalidad. Presuponiendo que estamos en un ámbito en el que el ánimo de lucro es inexistente, el tratamiento y análisis de los datos de tráfico sirve fundamentalmente para conocer el uso que tiene la red, tanto desde el punto de vista técnico —gestión de recursos y seguridad—, como humano —comportamiento del usuario—. Fines que pueden llevar aparejada la vigilancia de las actividades llevadas a cabo por los usuarios del sistema. No presenta grandes dudas la licitud del primer grupo de tratamientos al resultar necesarios para la prestación del servicio, (a la gestión del tráfico, la seguridad, o la detección de fallos y errores alude la directiva 2002/58 en varios de sus considerandos). Más problemáticos resultan los tratamientos orientados a verificar el uso de la red que hacen los usuarios.

Es sabido que tanto la RedIRIS [47] como las universidades [48] utilizan sistemas de control sobre las redes que gestionan. En España [49] su legitimidad se ha tratado fundamentalmente desde la perspectiva del derecho laboral. Es conocida la jurisprudencia, no del todo pacífica, que los legitima, fundamentándose

[47] Un ejemplo de sistema de captura y monotorización del tráfico que se ha utilizado en la RedIRIS es la Plataforma Mira. *Vid.* F. GALÁN et al., «MIRA: Plataforma de monitorización y análisis de tráfico para redes IP», en *http://greco.dit.upm.es/~abgarcia/publications/2003TELECOM.pdf.*

[48] Algunas universidades en sus Normas de Uso expresamente autorizan a la Administración de Recursos Informáticos a inspeccionar con carácter ordinario la información contenida en las cuentas de los usuarios. Si resulta necesaria una inspección más específica el administrador habrá de justificarlo y notificarlo a su superior. (*Vid.* Normas de la Universidad de Barcelona y las de la Universidad de León).

[49] En otros países de nuestro entorno el legislador ha optado por la elaboración de normas que específicamente observan la monotorización de las redes. Así, en el Reino Unido, la polémica *Regulation of Investigatory Powers Act, (RIP Act)* y su normativa de desarrollo, la *Telecommunication (Law Business Practice) (Interception Of Communication) Regulation*, aplicables a las instituciones educativas, permiten la monitorización de la red (y almacenamiento de los datos recabados) sin consentimiento de los usuarios cuando está orientada, entre otros motivos, a asegurar el cumplimiento de las normas de uso del sistema, investigar o detectar un uso no autorizado e incluso a detectar o prevenir la comisión de ilícitos penales, aun cuando el encargado del sistema ha de adoptar las medidas oportunas para asegurar que los usuarios conocen la existencia de estos mecanismos de control (*vid.* nota explicativa de la norma). Sobre la aplicación de estas normas en el ámbito educativo, cfr. B. WILLDER, «The Regulation of Investigatory Powers Act 2000», 2002, en *JISC Legal Informatin Service*, accesible en *http://www.jisc.ac.uk/uploaded_documents/lis_encryption_rip.pdf*, y del mismo centro el «Senior Management Briefing Paper 14: The Regulation of Investigatory Powers (RIP) Act 2000: Email and Telephone Monitoring», 2001, en *http://www.jisc.ac.uk/uploaded_documents/smbp14.pdf.*

en lo dispuesto por el artículo 20.3 del Estatuto de los Trabajadores (ET) [50] o en la Directiva 95/46, que autoriza algunos supuestos de monitorización del correo electrónico y del acceso a Internet del trabajador, siempre que se realice de conformidad con determinados requisitos [51]. En el entorno de las universidades no poseemos ni una norma de la naturaleza del ET ni, mucho menos, una ley orgánica que específicamente habilite la adopción por la Administración de «las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador (en nuestro caso los miembros de la comunidad universitaria) de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana» (*vid.* art. 20.3ET). No obstante, resultaría absurdo negar las facultades de supervisión y control sobre el funcionamiento de los servicios prestados y sobre el cumplimiento de los miembros de la comunidad universitaria de las condiciones del servicio, que ostenta la universidad en particular y la Administración en general, y que encuentra su fundamento último en el artículo 103 de la Constitución.

Identificados los intereses legítimos que posibilitarían *a priori* la adopción de algún tipo de control, es necesario llevar a cabo el juicio de proporcionalidad concretado en los siguientes aspectos: la *idoneidad* de la medida, —de modo que sea posible alcanzar el objetivo pretendido, (lo cual presupone la identificación clara del riesgo existente)—; su *necesidad,* —que no exista una medida menos gravosa o lesiva para la consecución del objetivo propuesto—; y la *proporcionalidad estricta,* —que el sacrificio del derecho reporte más beneficios al interés general que desventajas o perjuicios a otros bienes o derechos atendiendo a la gravedad de la injerencia y las circunstancias personales de quien la sufre—.

De acuerdo con estos extremos, antes de adoptar un mecanismo concreto de monitorización o control, deberá ser valorado a la luz de los tres puntos anteriores. Cabe diferenciar entre dos tipos de controles que comportarán un mayor o menor sacrificio de los derechos del afectado: los genéricos, que se lleven

[50] La base legal del artículo 20.3 ET como legitimadora de la restricción del secreto de las comunicaciones ha sido puesta en entredicho por la sentencia 402/2002 del Juzgado Social de Barcelona núm. 32 (AS 2002\2637), —que corrobora el TS de Cataluña en sentencia de 11 de junio de 2003 (AS 2003\2516)—, por carecer dicha norma del rango que determina el artículo 81.1 de la Constitución.

[51] *Vid.* en toda su extensión, Grupo de trabajo sobre protección de datos. Artículo 29. Documento de Trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Adoptado el 29 de mayo de 2002. 5401/01/ES/Final WP 55. Accesible en *http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_es.pdf.*

a cabo de manera sistemática sobre todo el flujo de la red para detectar la existencia de una disfunción o un peligro; y los excepcionales, relativos a una IP concreta, que necesariamente serán menos comunes y de mayor intensidad. En todo caso deberá evitarse el control sobre el contenido «sustancial» del mensaje —a saber, el contenido del mensaje o del archivo descargado—, por oposición a otros datos como la identificación de las IPs de destino, el momento de la conexión, o la extensión y el tamaño del archivo—. En tanto sea técnicamente posible, se deberán adoptar sistemas que discriminen los datos y el contenido de la comunicación, garantizando que la intromisión en el proceso de comunicación sea la adecuada. Asimismo se ha de partir de la filosofía de la prevención de modo que, con el debido respeto a la libertad de expresión, se puedan impedir determinadas transmisiones de datos o, al menos, insertar advertencias automáticas, antes que proceder a la interceptación del mensaje.

El correo electrónico es una herramienta especialmente sensible a cualquier sistema de vigilancia [52]. Por un lado porque la justificación de un mecanismo de control encuentra su fundamento en las potestades de supervisión y control que tiene la Administración sobre su red y, exclusivamente, sobre los miembros insertos en su organización. En el proceso de correo electrónico, intervienen terceros absolutamente ajenos, titulares igualmente de los derechos del artículo 18 de la Norma Fundamental, por lo que la instauración de mecanismos de control sobre el correo electrónico debería comunicarse en la medida de lo posible a sus destinatarios, mediante la inserción en todos los mensajes salientes de avisos advirtiendo de la existencia de sistemas de vigilancia. Por otro, porque determinados sistemas pueden afectar no sólo al continente, sino también al contenido del mensaje, sobre el que además existe una expectativa generalizada de privacidad. Ninguna de las justificaciones esgrimidas por el momento levantaría el secreto que ampara al contenido del mensaje, al existir, sin lugar a dudas, medidas menos restrictivas para alcanzar los fines perseguidos. Sólo la comisión de un ilícito penal podría llegar a motivar la apertura no automática de una cuenta, pero, en todo caso, la investigación de ilícitos no es ya una tarea propia de la Universidad, sino que corresponde a la Policía, que además, y en este supuesto en concreto, necesitaría la preceptiva autorización judicial.

[52] Sobre la interceptación de mensajes de correo electrónico en el ámbito de las instituciones de enseñanza superior, se ha pronunciado la Corte de Apelación de París que en la sentencia de 17 de diciembre de 2001, *caso Tareg,* consideró que los miembros encargados del sistema de comunicaciones que accedieron y divulgaron el contenido de los mensajes del correo electrónico de un investigador habían vulnerado su derecho al secreto de las comunicaciones.

El derecho a la intimidad, (y el artículo 10 de la Constitución) exige que la existencia de mecanismos de vigilancia sea conocida por los afectados. Hemos visto que aunque la herramienta básica de los mecanismos de vigilancia sea un tratamiento de datos relativo a las comunicaciones, ni el artículo 18.3 de la Constitución, ni la normativa de protección de datos —ni siquiera forzando la interpretación de la LGT o de la Directiva 2002/58—, ofrecen una base suficiente para requerir el consentimiento del afectado, que todo lo más vendrían a exigir una diligencia específica relativa al deber de información [53] (cuyo cumplimiento puede garantizarse con utilización de herramientas técnicas, p.e. a través de «ventanas informativas» que aparezcan en pantalla antes del uso del servicio o mediante la incorporación de la información en el formulario utilizado al solicitar los servicios), sin perjuicio de que la universidad decida *motu propio* recabar el consentimiento al no suponer éste grandes costes (bastaría un mero «clic»).

En todo caso ante controles dirigidos a analizar el cumplimiento de las obligaciones asumidas por los usuarios, es recomendable que se elaboren «Políticas de Información», adoptando medidas de publicidad que garanticen su conocimiento generalizado. En su formulación se ha de garantizar la participación de representantes de todos los miembros de la comunidad universitaria. Su contenido deberá incluir, como mínimo, los siguientes extremos [54]:

1. Descripción de los recursos informáticos que proporciona, detallando de forma pormenorizada en qué medida las diferentes categorías de usuarios pueden utilizar los sistemas y servicios de comunicación con fines personales.
2. Los motivos, la finalidad, y los diferentes tipos de controles. Al admitir que existe una tolerancia hacia el uso personal los controles debería tener un carácter muy limitado. Se deberá relacionar claramente qué datos derivados de un control sistemático de poca intensidad comportarán un control más intenso.
3. Información detallada sobre las medidas de vigilancia, ¿quién?, ¿cuándo? y ¿cómo? las adopta.
4. Información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los usuarios en caso de infracción de las

[53] Sobre el deber de informar de la LOPDCP, *vid.* en este mismo volumen P. GRIMALT, Capítulo VIII, apdo. 3.2.

[54] Se han adaptado los criterios expuestos por el Grupo del artículo 29 al ámbito de las universidades en Documento de trabajo relativo a la vigilancia de las comunicaciones... ref. en nota 51.

normas de uso y de los medios que disponen para reaccionar en estos casos. Se debería informar inmediatamente al usuario de cualquier abuso detectado.

Cabe destacar que, a diferencia del Reino Unido [55], nuestro ordenamiento no permite, salvo que medie consentimiento, la utilización sistemática de controles para detectar la comisión de actos ilícitos por parte de los usuarios. Por otro lado entiendo que los deberes de denuncia impuestos por la Ley de Enjuiciamiento Criminal ceden ante el deber de secreto profesional de la LOPDCP, a no ser que se haya informado y consentido al respecto. Es más, la especial configuración del secreto de las comunicaciones prohíbe la comunicación de los datos a personas ajenas a la comunicación, salvo, eso sí, autorización judicial. Mientras no se desarrolle el artículo 12, los datos de tráfico ni siquiera podrán ser comunicados a la Policía o al Ministerio Fiscal [56], al prevalecer el artículo 18.3 de la Constitución sobre la normativa de protección de datos.

Ya por último el artículo 13 de la LOPDCP prohíbe la sanción automática (por ejemplo la denegación de un servicio para un usuario determinado) fundamentada en la información derivada exclusivamente del tratamiento de datos. El centro deberá previamente advertir de esta finalidad a los posibles afectados [57], además de, en congruencia con el principio de contradicción, dar audiencia al interesado. Si no se publicado la existencia del fichero o aún haciéndolo, no se ha señalado tal finalidad, no se podrá imponer ningún tipo de medida sancionadora, incurriendo tanto la universidad como probablemente los encargados del tratamiento en una infracción de la normativa.

f) *Espacios privados en el entorno virtual*

En el mundo virtual existen ciertos espacios de carácter más o menos privado, cuyo acceso por un tercero, puede considerarse una injerencia no autorizada por el ordenamiento. La amplitud del derecho a la intimidad dependerá de las expectativas que tenga el usuario, que variarán en función del tipo de servicio. Así para determinados servicios como el *ftp* público o las listas de distribu-

[55] *Vid.* nota 48.

[56] En el mismo sentido *vid.* Circular de la Fiscalía del Estado 1/1999 (RCL 2000, 876) y F.H. HERNÁNDEZ, *op. cit.* nota. 35.

[57] Sobre el artículo 13 LOPDCP, *vid.* M. VIZCAÍNO, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal,* Madrid, 2001, págs. 183 y ss.

ción, las expectativas de privacidad aparecen naturalmente mermadas, por lo que el acceso a los datos almacenados no puede interpretarse como intromisión ilegítima en la intimidad de los usuarios. Los servicios más afectados serían el correo electrónico (*vid.* supra) o los espacios privados de alojamiento de datos, localizados en uno de los servidores de la universidad (*ftp* privado) o en el ordenador del usuario.

Tanto el acceso a los ordenadores como el acceso a los archivos de la cuenta *ftp* que no cumplan con el juicio de proporcionalidad anteriormente enunciado merecen un reproche legal. En contra de lo que han venido sosteniendo algunos tribunales considero que la mera titularidad de los bienes no otorga potestad suficiente para registrar los recursos de los que disfruta el usuario. Ni siquiera el conocimiento de que terceros, miembros del equipo de comunicaciones, tienen las facultades técnicas para acceder a la máquina, diluyen la expectativa de privacidad de los usuarios.

Finalmente, y ante las dudas que en la práctica tendrá que afrontar el departamento de servicios de informática, el encargado del sistema ha de tener presente el principio de *favor libertatis*, aun tratándose de relaciones de especial sujeción [58]. No olvidemos que al dictado del artículo 27 de la Constitución *«la educación tendrá por objeto el pleno desarrollo de la personalidad humana en el respeto a los principios democráticos de convivencia y a los derechos y libertades fundamentales»,* principios que deberán informar todo el actuar de la institución universitaria, por lo que la tentación de cualquier restricción, por legítimo que su fin sea, a las libertades de los miembros de la comunidad universitaria ha de tomarse con extremadísima cautela.

4. LA RESPONSABILIDAD PATRIMONIAL DE LAS UNIVERSIDADES PÚBLICAS

4.1. Introducción

La delimitación del régimen de responsabilidad de las universidades públicas en su rol de intermediarias es un tema conflictivo debido al carácter objetivo y directo de la responsabilidad de la Administración y al alcance del término «neutralidad tecnológica». Anunciaba al principio que mi objetivo era proporcionar herramientas que facilitaran la exoneración de responsabilidad de las uni-

[58] Como ha destacado M. LÓPEZ BENÍTEZ, en su obra *Naturaleza y Presupuestos Constitucionales de las Relaciones Especiales de Sujeción,* «...la fuerza expansiva de los derechos fundamentales despliega todavía una importante función... Se trata de que esta interpretación a favor

versidades por los daños lesivos causados por miembros de la comunidad universitaria. Matizaré esta afirmación, sólo por los actos lesivos que impliquen un uso personal o particular del servicio [59].

A lo largo de esta obra se han estudiado los presupuestos de irresponsabilidad dispuestos por los artículos 14 y ss de la LSSICE. Hemos visto que en la mayoría de los casos se trata de una exoneración por hechos ajenos. ¿Pueden considerarse «ajenos» los miembros de la comunidad universitaria? También hemos visto que las universidades suelen controlar el uso de la red, ¿suponen estos controles una ruptura de la neutralidad tecnológica?

4.2. La responsabilidad patrimonial de la Universidad por la mera provisión de contenidos. La aplicación del régimen general

Continuamente se ha hecho referencia a los servicios de intermediación, por lo que resultaría obvio comenzar el análisis de responsabilidad refiriéndonos a esta actividad. Sin embargo hay casos en los que dicho análisis pudiera parecer innecesario, especialmente cuando el origen de los datos transmitidos o alojados por la universidad se remonte al personal inserto en su organización, es decir, casi siempre. Ello merece una breve reflexión sobre la responsabilidad de la Administración por la mera provisión de contenidos [60]. Cabe distinguir entre

de los derechos fundamentales obliga a restringir el alcance de las normas limitadoras que actúan sobre los derechos fundamentales, previsión que no creemos pueda sufrir merma con respecto a las relaciones especiales de sujeción», pág. 407, *op. cit.*, Madrid, 1994.

[59] No se tratará la responsabilidad por el ejercicio de la actividad de copia temporal, regulada en el artículo 15 LSSICE, al considerar que la mayoría de supuestos subsumibles en el precepto no se refieren tanto a acciones dañosas llevadas a cabo por miembros de la comunidad universitaria distintos del intermediario, —aunque no son extrañas al precepto—, sino que más bien son infracciones del propio intermediario por el incumplimiento de los deberes que la naturaleza de la actividad exige y que por lo tanto implican responsabilidad por hecho propio. *Vid.* en esta misma obra S. CAVANILLAS, Cap. II, apdo. 3. Otros supuestos de responsabilidad por hecho propio se derivarían del incumplimiento de las normas relativas a seguridad (*vid.* MORALES, O., «Criterios de atribución de la responsabilidad penal a los prestadores se servicios e intermediarios de la sociedad de la información», en F. MORALES/O. MORALES (coord.), *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet,* Cizur Menor, 2002, pág. 187).

[60] Para evitar confusiones, ya que en la práctica es difícil distinguir entre la actividad de intermediación y la de provisión de contenidos, durante la lectura de este apartado en algunos casos resultará útil imaginar que la actividad de intermediación la realiza un tercero distinto de la universidad, que pone a disposición de ésta sus infraestructuras para que los miembros de la comunidad universitaria las utilicen. La utilización que lleven a cabo los miembros de la institución podrá estar relacionada con el servicio público de la educación superior o podrá adscribirse a un uso personal o particular de los destinatarios. La cuestión está en determinar si la universidad sería responsable de la ilicitud de los datos que los usuarios le solicitan al intermediario ajeno a la estructura universitaria que transmita o que aloje. Otras veces esta comparación más que facilitar el análisis de responsabilidad lo complica, principalmente cuando se haga referencia a instrumentos de supervisión o control, ya que en el ámbito de la provisión de contenidos, y exceptuando la improbable aparición de una figura intermedia que se dedique a autorizar los datos antes de remitírselos al intermediario, la posibilidad cierta de hacer efectivos mecanismos de supervisión y control es a través de herramientas técnicas interpuestas por el intermediario.

contenidos claramente institucionales, (como los publicados en la página web de la universidad o en el marco de la enseñanza en línea) y los contenidos transmitidos o alojados que, pese a ser transmitidos o publicados utilizando los servicios de intermediación de la universidad y por miembros integrados en su esfera organizativa, no necesariamente constituyen una manifestación, siquiera aparente, de la actividad de servicio público, sino más bien una manifestación de un uso particular o personal. El primer supuesto no presenta problema alguno, la universidad proveedora de contenidos responderá por la ilicitud de éstos. Pero, en relación con el segundo ¿es igualmente responsable?, ¿qué argumentos podrá esgrimir para excusar su responsabilidad?

La apreciación de responsabilidad tendría como consecuencia un régimen muy estricto de control sobre el uso de la red, control que además de costoso podría implicar una importante restricción de servicios que tanto han contribuido a la «alfabetización digital», a la difusión de conocimientos y a una acceso igualitario a la red. El régimen de responsabilidad objetiva y directa por lesiones producidas como consecuencia del funcionamiento normal o anormal de los servicios públicos que ha impuesto el legislador a la Administración (arts. 139 y ss de la LRJAP) no es un lecho confortable para defender su irresponsabilidad. Veamos cuáles son los requisitos de este régimen e intentemos descifrar en qué casos la universidad respondería o no por los datos que los usuarios transmiten o incorporan a la red.

Además de la existencia de un daño evaluable económicamente que el perjudicado no tenga la obligación de soportar (1), son presupuestos necesarios para apreciar la responsabilidad de la Administración que la lesión no provenga de fuerza mayor o de los denominados riesgos de desarrollo y que sea consecuencia del funcionamiento normal o anormal de los servicios públicos (2), y que exista una relación de causa-efecto entre la actividad administrativa a la que se achaca el daño y el resultado lesivo (3). Por otro lado el ámbito subjetivo de la

responsabilidad requiere la integración del agente del daño en la organización administrativa y que el daño halle su origen en el ejercicio o con ocasión de las funciones públicas que a tal agente le han sido asignadas (4).

Partiendo del análisis del ámbito subjetivo, generan responsabilidad los actos causados por agentes integrados en la estructura administrativa o, en determinados casos, por agentes autorizados por la Administración. En cambio los actos de los particulares, usuarios de un servicio público, que causen lesiones a terceros con ocasión del funcionamiento normal del servicio no suelen implicar la responsabilidad de la Administración. La particularidad de nuestro objeto de estudio es que en determinados supuestos los proveedores de contenidos son al mismo tiempo usuarios de un servicio público y Administración, al estar insertos en su estructura organizativa, bien en virtud de vínculos funcionariales o laborales (el PDI y el PAS), bien por razón de una relación de especial sujeción (alumnos).

El segundo presupuesto subjetivo requiere que el daño sea causado en el ejercicio de las funciones públicas o con ocasión de las mismas. Así se excluye la responsabilidad de la Administración por aquellos actos «puramente personales del sujeto al servicio de la Administración pública realizados con desconexión total del servicio» [61]. Este requisito resulta especialmente relevante en el ámbito que nos ocupa.

En primer lugar porque no alcanza al uso personal o particular que la Administración especialmente tolera y que viene a confirmarse como una actividad en desconexión total de las funciones que el agente tenga encomendadas

[61] J.M. BUSTO, en «La responsabilidad civil de las Administraciones Públicas» en REGLERO, (coord.) *Tratado de Responsabilidad Civil*, 2.ª ed., Cizur Menor, 2003, pág. 1564.

En el mismo sentido, GARCÍA DE ENTERRÍA, *Curso de Derecho Administrativo*. II 8.ª ed., Madrid 2002, pág. 399, que incluye una referencia expresa a la Sentencia del Tribunal Supremo (Sala de lo Contencioso-Administrativo), de 20 mayo 1986, parte de cuyo Fundamento de Derecho Primero se reproduce a continuación : «lo que si resulta patente es la improcedencia de la reclamación de una indemnización por unas lesiones atribuibles a unos servidores del Orden Público por unas acciones cometidas sin relación alguna con el ejercicio de su función; procediendo afirmar que no puede declararse la responsabilidad del Estado por las acciones u omisiones imputables a autoridades o funcionarios que hayan ocasionado una lesión en los bienes o derechos de los particulares, cuando su conducta, dolosa o culposa, no se corresponda con el ejercicio de esa autoridad o función que sea inherente a un Servicio Público, pues, en este supuesto, falta el nexo de causalidad exigido por el artículo 40 de la Ley de Régimen Jurídico del Estado, acorde con el 106-2 de la Constitución entre la conducta de un agente que actúa en el ejercicio de una potestad o función pública y el daño causado, ya que no se puede responsabilizar al Estado lo que se haga u omita por un particular, o por quien esté revestido de autoridad o sea empleado público pero obre al margen de esa condición, y por ello sin relación alguna con el funcionamiento normal o anormal de un Servicio Público».

por razón de los vínculos que le unen con la Administración. En este caso el miembro de la comunidad universitaria actúa como un particular, siendo responsable de la actividad que lleve a cabo. Así, entiendo que cuando la universidad autoriza la utilización de correos electrónicos con fines privados o el alojamiento de páginas web personales, realmente está prestando un servicio del mismo modo que lo hace cualquier Administración en relación con sus administrados. En la causa de la acción prima el disfrute del servicio frente a la función que el destinatario ejerce en la Administración.

En segundo lugar, su ausencia se observa a aquellos supuestos en los que aun existiendo una prohibición sobre el uso personal, el sujeto integrado en la estructura de la Administración realiza una utilización del servicio que responde sólo a intereses privados y presenta una apariencia de desconexión total con la prestación del servicio público. Pensemos por ejemplo en el envío de correos electrónicos con contenidos ilícitos por un alumno o en los datos alojados en los discos duros virtuales del servidor del centro cuyo uso (sobre el que recaen además ciertas expectativas de privacidad) es generalmente privativo del profesor al que se le asigna.

Finalmente cabe analizar el alcance de las relaciones de especial sujeción, es decir el despliegue de las facultades especialísimas que la Administración puede ejercer sobre el administrado y que vendrían indirectamente a coincidir con la oportunidad y las potestades de supervisión y control y con la esfera de responsabilidad de aquella. En primer lugar las potestades de supervisión y control no son ilimitadas, sino que especialmente en el ámbito de la universidad se han de conjugar con el ámbito funcional en el que se ejercen y con ciertos derechos y libertades de los que deben disfrutar los estudiantes. Las universidades no son responsables de *todo* lo que hagan sus alumnos mayores de edad, aun cuando lo hagan en sus instalaciones o en virtud de las prerrogativas que el hecho de ser miembro de la comunidad universitaria les proporciona. Igualmente cabe destacar que cuando la jurisprudencia ha apreciado responsabilidad de la Administración por actos realizados por quienes están sujetos a una relación de especial sujeción la ha reconducido al funcionamiento anormal de los servicios públicos al apreciar falta de diligencia de la Administración, subjetivizando la responsabilidad de la Administración al incidir en sus deberes de vigilancia o de cuidado respecto de aquellos ante los que se instituye en una posición de garante [62].

[62] Entre otras sTS de 13 de marzo de 2001 (RJ 2001\1382), en la cual se observa la responsabilidad de la Administración penitenciaria por el apuñalamiento de un preso a manos de otro

Por otro lado desde hace algunos años se ha intuido tanto en el ámbito normativo como en el jurisprudencial y doctrinal cierta relajación de la teoría objetiva. En relación con el primero cabe recordar las modificaciones de la Ley 4/1999 que introducen los riesgos de desarrollo como causas de exoneración de la responsabilidad. Desde entonces, no sólo se admite la exoneración de responsabilidad en supuestos de fuerza mayor sino también cuando «los daños se deriven de hechos o circunstancias que no se hubiesen podido prever o evitar según el estado de los conocimientos o de la técnica existente en el momento de la producción de aquellos» [63].

Por su parte, tanto la jurisprudencia como parte de la doctrina han defendido, a veces frontal y otras indirectamente, cierta atenuación de los restantes presupuestos de la responsabilidad [64]. En el ámbito de las actividades educativas son varias las sentencias del Tribunal Supremo que han exonerado de responsabilidad a la Administración por hechos acontecidos durante la realización de actividades educativas o en instalaciones escolares, matizando la aplicación de los conceptos de funcionamiento normal y anormal del servicio e introduciendo en sus Fundamentos de Derecho alusiones ajenas al régimen objetivo de la responsabilidad, como el caso fortuito [65] o los deberes de diligencia. Por su puesto todas ellas se refieren a ubicaciones o manifestaciones del mundo físico, pero nada, en principio, obsta para aplicar los razonamientos expuestos al entorno virtual.

Entre las más recientes, la sentencia de 13 de septiembre de 2002 (RJ 2002\8649), que deniega el derecho al reconocimiento de una indemnización por responsabilidad de la Administración derivada de la muerte de un alumno que practicaba una actividad deportiva, al apreciar la ausencia del nexo causal derivado de un hacer o falta de hacer de la Administración y el desgraciado accidente. Se hace referencia a lo largo de la sentencia a varios pronunciamientos del mismo Tribunal, coincidentes en la idea de que el uso de instalaciones o, en especial, de la infraestructura material para la prestación de un servicio público, no implica o convierte a la Administración en responsable de todos los resultados lesivos que puedan producirse por su uso, sino que es necesario que los daños sean consecuencia directa e inmediata del funcionamiento normal o anormal del servicio.

Hay un último argumento que nos lleva a insistir en la exención de responsabilidad de la Administración por actos realizados por el personal a su servicio o los alumnos del centro en supuestos de usos con fines particulares. La afirmación a priori de responsabilidad en el ámbito que nos concierne implicaría el ejercicio de un control rigurososísimo el cual, so pena de rozar la censura, se constituye en una carga costosa y no demasiado eficiente, que, como contrapartida, llevaría aparejados unos riesgos económicos nada despreciables (no hay más que pensar en las cuantiosas sumas que la RIAA reclama por la distribución de sus películas). Ello hace más que probable la adopción de medidas preventivas que podrían llegar a alcanzar la prohibición absoluta de cualquier uso personal de los servicios de intermediación e incluso, en algunos supuestos, la prohibición de uso sin más, lo cual es absolutamente indeseable [66].

interno al apreciar «falta de la debida diligencia (de la Administración), la cual, sobre suponer el incumplimiento de los particulares deberes que al respecto impone la normativa penitenciaria, fue la determinante de la mortal agresión causada».

[63] Art. 145.2 LRJAP. Si bien puede afirmarse que acreditar la inevitabilidad de los daños por parte de la Administración universitaria es harto difícil, al requerir un control sobre la actividad de intermediación muy costoso tanto en términos económicos como técnicos —sin mencionar el sacrificio probablemente innecesario de los derechos y libertades de la comunidad universitaria—, ésta dificultad no puede subsumirse en la causa de exoneración de responsabilidad relativa a los riesgos de desarrollo, al depender éstos del estado de los conocimientos científicos y técnicos.

[64] M. ATIENZA ha criticado las consecuencias de la aplicación de la responsabilidad objetiva y directa en el ámbito de los centros docentes públicos, en *La responsabilidad civil por los hechos dañosos de los alumnos menores de edad*, Granada, 2000, págs. 252 y ss.

[65] Se alude al «hecho fortuito» y al «golpe fortuito» en la sTS de de 24 julio 2001 (RJ 2001\5410) que exonera de responsabilidad a la Administración docente por las lesiones causadas a uno de sus alumnos por una patada de un compañero. Vale la pena mencionar que la sentencia trae a colación el artículo 1903 del Código civil que recordemos dispone que «Las personas o entidades que sean titulares de un centro docente de enseñanza no superior responderán por los daños y perjuicios que causen sus alumnos menores de edad durante los períodos de tiempo en que los mismos se hallen bajo el control o vigilancia del profesorado del centro, desarrollando actividades escolares o extraescolares y complementarias».

[66] Recordemos el razonamiento esgrimido en la sentencia de la Sala de la Jurisdicción del Tribunal Superior de Justicia de Cataluña de 22 de junio de 1999 (RJCA 1999, 1644), —reproducido en la sTS de 13 de septiembre de 2002—, en la que haciendo referencia a la actividad deportiva en el marco de la cual se causaron los daños entiende que «la actividad en sí misma no puede calificarse de peligrosa y que, en la práctica, era incontrolable pues, para hacerlo, sería necesario adoptar medidas que significarían «de facto» la prohibición de esa clase de juegos cuya práctica es necesaria para el normal desarrollo de la personalidad de esos jóvenes; decisión que no sería razonable y que obviamente resultaría desproporcionada y atentaría derechos básicos de los jóvenes». En el ámbito que nos ocupa el uso de la red ha sido un importante instrumento para cubrir las necesidades de educar y acostumbrar a la comunidad universitaria (y no sólo a los alumnos) en la utilización de las herramientas informáticas (aún hay gente que no tiene ordenadores y mucho menos conexiones adsl o tarifas planas que le permitan un uso óptimo de la red). Además no podemos olvidar que la red es un espacio extremadamente idóneo para el desarrollo de las capa-

Al igual que no resulta congruente exigirle a la Administración responsabilidad por los datos que transmiten o alojan los usuarios de las estructuras de red proporcionadas por un ayuntamiento [67], tampoco parece adecuado exigirle responsabilidad a la universidad por el uso personal que los alumnos e incluso el PDI o el PAS hace de los servicios prestados, especialmente cuando no existe (ni, salvo en determinados casos, resulta pertinente) una actividad de vigilancia sobre la provisión de contenidos o cuando en el caso de existir la intensidad de la misma está limitada, por razones obvias, a supuestos muy concretos.

Puede afirmarse en este sentido que los riesgos que presentan ciertas actividades desarrolladas en el marco de la prestación de un servicio público, y en especial la autorización para el alojamiento de páginas o transmisión de datos a través de la red propia o la actividad de intermediación, son riesgos permitidos o asumidos socialmente cuya manifestación cristalina es la exoneración de responsabilidad en las actividades de intermediación. En todo caso no hay que olvidar que la no aplicación de la responsabilidad prescrita por los artículos 139 y ss LRJAP no implica en absoluto la denegación del derecho a la reclamación del perjudicado, ya que éste si bien no podrá obtener el oportuno resarcimiento de la universidad podrá, por su puesto, dirigirse contra el verdadero responsable, es decir el autor del acto lesivo.

Asimismo cabe recordar que cuando el acto lesivo esté directamente relacionado con la actividad académica del causante, entonces no habrá dudas sobre la aplicación del régimen de responsabilidad previsto por la LRJAP, al coincidir probablemente el supuesto de hecho con la actuación de la universidad como proveedora de contenidos o con un funcionamiento anormal del servicio prestado. Cuando la universidad ha asumido dentro de los límites constitucionales, un deber de supervisión y control sobre la actividad ejercida por el usuario, y el incumplimiento de este deber coadyuva a la producción del daño (es decir si éste se hubiera podido evitar), entonces no habrá razón para exonerarla de responsabilidad por el funcionamiento anormal de sus servicios. Sin embargo habrá de tenerse en cuenta que la mayoría de los controles operarán una vez que el daño ha comenzado a producirse, por lo que sólo resultarían imputables a la Administración los daños producidos desde el momento en que ésta ha podido actuar y no lo ha hecho. La responsabilidad podrá imputarse exclusiva de la Administración, que deberá repetir contra el causante, o, en los supuestos en los que se advierta un uso particular o personal de los servicios, concurrente de la Administración y del agente creador del daño. A tenor de los dispuesto por el art. 9.4 de la LOPJ deberá conocer de las pretensiones del perjudicado la jurisdicción contencioso-administrativa.

cidades de la comunidad universitaria y en especial el ejercicio de algunas de sus libertades y derechos, la libertad de expresión, de estudio, de investigación y cátedra y el derecho a la información, tanto en su vertiente activa como pasiva.

[67] *Vid.* en esta obra, J. VALERO, Capítulo VI, apdo. 3. Cabe destacar que el autor (previsiblemente en contra de lo que se ha venido exponiendo) considera que cuando el centro «proporcione el alojamiento a los destinatarios de un servicio público como parte de las actividades en que consista su ejecución, tal y como sucede singularmente en el caso de los alumnos de un centro educativo... la Administración Pública asumiría directamente los daños causados a terceros dado que, en definitiva, su posición jurídica le otorga una potestad de supervisión y control respecto de cualquier actividad que aquellos lleven a cabo con ocasión de la prestación del servicio público de que se trate: no resulta, por tanto, tan relevante el hecho de la efectiva incorporación del agente a la esfera administrativa como la constatación de que haya sido el funcionamiento de los servicios públicos la causa que, directa o indirectamente, haya producido los perjuicios, tal y como sucede singularmente en este caso».

4.3. La responsabilidad de la Universidad como proveedora de los servicios de intermediación

A. *Servicios de acceso o transmisión de datos*

La exoneración del artículo 14 LSSICE opera cuando los prestadores no han originado la transmisión, modificado o seleccionado los datos o seleccionado a los destinatarios. Es decir, la universidad no responderá cuando no provoque la ruptura de su neutralidad tecnológica.

Como hemos visto tanto las universidades como la RedIRIS implementan sistemas que, en mayor o menor medida, y, con mayor o menor intensidad, controlan los datos e incluso llegan a seleccionarlos con el fin de evitar su transmisión, (bloqueando por ejemplo la transmisión de archivos infectados). Entiendo que este tipo de sistema de control no desvirtúa el papel de intermediario que ejercen los prestadores. La selección a la que hace referencia el legislador parece exigir un papel activo por parte del prestador, que ponga de manifiesto la intencionalidad de transmitir ese contenido en concreto a la red [68]. En los casos en los que los mecanismos de control se instituyan para evitar la transmisión de determinados contenidos, y éstos no son detectados por el mecanismo de filtrado, entonces podría llegar a incurrirse en responsabilidad por la falta de diligencia del proveedor al realizar la selección.

[68] *Vid.* al respecto en este volumen S. CAVANILLAS, Capítulo III, apdo. 2.

En segundo lugar, y a diferencia de lo prescrito por artículos siguientes, el artículo 14 configura una exención de carácter objetivo [69], en tanto no hace depender la responsabilidad del intermediario del conocimiento efectivo que éste pudiera tener respecto de los contenidos ilícitos que se transmitan a través de su red. La ausencia de un deber de diligencia, a diferencia del establecido en el artículo 16, tiene como consecuencia que si la universidad tuviera conocimiento de que se están cometiendo ilícitos a través de su red, no se le exija, *ex* LSSICE y dentro de los límites referidos en el considerando 44 de la DCE [70], que tome las medidas oportunas y técnicamente a su alcance para cesar las transmisiones ilícitas o bloquear el acceso a los contenidos transmitidos.

Ello ha entenderse sin perjuicio de la aplicación, en su caso, de los deberes de denuncia impuesto por la Ley de Enjuiciamiento Criminal o, especialmente y en el ámbito que nos ocupa, el artículo 19 del RD 898/1985 [71], que condicionan la respuesta que ha de dar el conocedor del ilícito o de la falta disciplinaria (salvo que medie deber de secreto), so pena de incurrir en responsabilidad.

La ausencia de un deber de diligencia en la LSSICE no deroga ni las normas citadas ni los compromisos que asuma reglamentariamente la universidad respecto de los servicios específicos de intermediación, de modo que cuando en sus normas internas de funcionamiento se disponga el deber de reacción ante la comisión de determinados actos, y siempre que su ejercicio no implique la colusión de otros derechos fundamentales, el centro se verá obligado a adoptar las medidas oportunas y técnicamente a su alcance para impedir el mantenimiento del acceso o la transmisión de datos de cuyo carácter ilícito tiene conocimiento efectivo. La omisión del cumplimiento de los deberes de reacción asumidos unilateralmente podría dar lugar a responsabilidad por el funcionamiento anormal del servicio.

[69] M. PEGUERA, «La exención de responsabilidad civil por contenidos ajenos en Internet» en F. MORALES/ O. MORALES (coords.): *Contenidos Ilícitos y Responsabilidad de los Prestadores de Servicios de Internet,* Cizur Menor 2002, págs. 40 y ss.

[70] «Un prestador de servicios que colabore deliberadamente con uno de los destinatarios de su servicio a fin de cometer actos ilegales rebasa las actividades de mero transporte (mere conduit) o la forma de almacenamiento automático, provisional y temporal, denominada "memoria tampón" (caching) y no puede beneficiarse, por consiguiente, de las exenciones de responsabilidad establecidas para dichas actividades».

[71] «Las autoridades académicas, sea cual fuere su rango o cargo, que *toleren* o encubran la realización de actos o conductas constitutivas de falta disciplinaria, incurrirán en responsabilidad y se procederá a las actuaciones previstas en el ordenamiento jurídico para su corrección».

B. *Alojamiento*

La exoneración de responsabilidad del artículo 16 LSSICE no opera «en el supuesto de que los destinatarios del servicio actúen bajo la dirección, autoridad o control de su prestador». En una primera acepción, el artículo parece referirse a la responsabilidad por hecho ajeno en el marco de una relación de dependencia o, en nuestro caso concreto, a la responsabilidad de la Administración por las acciones del personal a su servicio (incluyendo a los alumnos) en el ejercicio de sus funciones o con ocasión de las mismas. Una vez más, resulta necesario delimitar si los miembros de la comunidad universitaria por el mero hecho de hacer uso de los servicios que la universidad pone a su disposición están actuando bajo su dirección, autoridad o control. Ya hemos visto que por un lado se da un amplio margen de tolerancia sobre la utilización personal de los servicios, lo cual sugiere la ausencia de control en estos ámbitos, y, por otro, que existen unos límites constitucionales sobre el control efectivo que la universidad puede ejercer sobre la actividad de los destinatarios; por lo que aquellas acciones que se excedan ética y legalmente de su ámbito de control y que además no guarden relación o apariencia alguna con el ejercicio de las funciones atribuidas al personal, no se adecuan a lo previsto en el artículo 16.2.

Pero además, tal y como entendieron los antecedentes jurisprudenciales que informaron la directiva 2000/31 y las reformas de la legislación estadounidense, el espíritu del artículo 16.2 no es sólo un trasunto de aquellas normas que específicamente se refieren a las relaciones de dependencia o de especial sujeción, sino que hace referencia al control que el intermediario ejerza sobre la actividad concreta de provisión de contenidos, control que se derivará de las obligaciones asumidas por el servicio prestado. Así si éstas otorgan al intermediario el derecho o el deber de controlar los contenidos incorporados a los espacios por él cedidos se deroga la regla especial de responsabilidad prevista en el artículo 16.1 [72]. En qué medida un tipo de control concreto tiene la entidad suficiente para derogar la regla especial de responsabilidad merece un análisis del caso concreto [73] en relación con los aspectos subjetivos del control [74].

[72] En relación con la DCE, I. GARROTE, «La responsabilidad civil extracontractual de los prestadores de servicios en línea por infracciones de los derechos de autor y conexos», *Pe. I. : Revista de Propiedad Intelectual.* núm. 6, sep.-dic. 2000, Madrid, pág. 49 in fine.

[73] Un caso típico en la provisión de alojamiento es el de los foros de noticias moderados. El hecho de que el foro esté moderado y que el moderador tenga en consecuencia cierto control sobre cada uno de los mensajes incorporados a la red no es razón suficiente para exigirle responsabilidad por todos los mensajes insertos en el foro, especialmente por aquellos en los que se

Entrando ya en el análisis del apartado primero del artículo 16, se establece que la universidad no incurre en responsabilidad cuando no tiene conocimiento efectivo de que la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o, si lo conociere, procede a su bloqueo o retirada. Esta vez sí entra en juego el deber de retirada de la información [75].

El artículo enuncia una lista abierta del origen del conocimiento. En el caso que nos ocupa presentan especial relevancia los controles (procedimientos de detección) llevados a cabo por el prestador de servicios y las notificaciones enviadas por terceros alertando de la existencia de material ilícito.

La alusión a los «procedimientos de detección» presenta cierta imprecisión sin duda potencialmente contraria al espíritu del artículo. Los sistemas de detección presuponen un control *a posteriori* de los datos alojados en los espacios del prestador, lo cual podría caer, —pese a lo dispuesto en el considerando 40 de la Directiva—, en el ámbito del artículo 16.2, o, en todo caso, dependiendo de la configuración de estos controles, originar la existencia de un deber de detección de los ilícitos alojados en los servidores [76]. Salvando esta apreciación, queda claro que si la universidad hubiera puesto en marcha controles relativos a la detección de ilícitos (cuya licitud en algunos casos pudiera ser más que cuestionable) y éstos identificaran alguna acción manifiestamente prohibida por la ley deberán proceder a la retirada de los materiales alojados. Cabe señalar que

hace prácticamente imposible dilucidar la ilicitud del contenido. Por ello, la regla dispuesta por el artículo 16.2 no debe entrar en juego de manera automática en tanto sus efectos son de los más perniciosos: o se elimina el control sobre cualquier grupo de noticias, lo cual evidentemente en el ámbito de la universidad impediría cualquier tipo de discusión centrada y específica sobre un tema, o se contrata a una comité de expertos encargado de verificar la licitud de todos los mensajes incorporados al foro.

[74] En este sentido se ha pronunciado la jurisprudencia estadounidense en el caso *Ezra v. AOL,* sentencia de la Corte de Apelación (10th Cir.) de 14 de marzo de 2000, en el que pese a apreciar que el proveedor de alojamiento había ejercido algún tipo de control sobre el contenido, en concreto, y varias veces, comunicando correcciones a los proveedores de contenidos e incluso borrando parte de la información creada por éstos (realmente se limitaba a eliminar símbolos relativos a la información para hacerla inaccesible), no podía ser considerado igualmente proveedor de contenidos al no ser ni su creador ni su desarrollador.

[75] El deber de retirada de información ha sido tratado en detalle por S. CAVANILLAS, Cap. II. apdo. 2 de esta obra.

[76] Ya hemos visto que el establecimiento de mecanismos de detección de ilícitos por parte de la universidad, consistiría en sí mismo un actividad administrativa, que, dentro de los límites impuestos por el estado de la técnica, podría dar lugar a responsabilidad.

de los resultados de los controles relativos a la detección de flujos de datos o gestión del espacio no necesariamente se deriva la ilicitud de la actividad [77].

¿Puede entenderse que las notificaciones de terceros, distintos de la autoridad judicial, son una fuente de conocimiento efectivo? El alcance del concepto de conocimiento efectivo, ha sido tratado por S. CAVANILLAS [78] en este mismo volumen. Siguiendo sus conclusiones entiendo que la LSSICE no le está exigiendo a los servidores que reaccionen valorando la licitud de los datos y retirándolos, especialmente a falta de un procedimiento de comunicación como el establecido por la DMCA [79] que le exonere de la eventual responsabilidad que puede suponer la retirada de información lícita [80]. Sin embargo, tengo mis dudas sobre, si atendiendo a las especiales características de la relación entre la universidad y los usuarios del sistema, no resultaría pertinente exigirle a ésta, no en virtud de la LSSICE sino por razón de sus facultades de supervisión, que adoptara las medidas adecuadas para constatar la ilicitud de los datos y si ésta fuera evidente los retirara.

En el caso de que la universidad valore la notificación y efectivamente proceda a la retirada de los datos o a la suspensión del servicio, tales actuaciones

[77] A título de ejemplo el conocimiento de la institución de que en sus servidores (o en su caso en los ordenadores de los usuarios que se configuran como tales) existen archivos mp3 no debería ser considerado conocimiento efectivo ni simple conocimiento, aún cuando la experiencia la admita como probable, de que se está albergando información protegida por los derechos de autor. En el mismo sentido. COOPER, C. «Legal Risks and Liabilities for IT Services in Higher and Further Education», pág. 6 en *http://www.jisc.ac.uk/uploaded_documents/Risk_IT_Cooper.pdf* .

[78] Apdo. 2.4, Capítulo II de esta obra.

[79] Aún en EEUU, y pese a la existencia de los procedimientos de notificación bastante definidos, se ha puesto de manifiesto un uso abusivo por los titulares de derechos de autor del sistema previsto en la sección 512(c) de la *Copyright Act*. *Vid.* la nota «Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands» publicada en la página web de la Electronic Frontier Foundation, *http://www.eff.org/IP/P2P/20030926_unsafe_harbors.php*. El sistema de *notice and take down* constituye una importante herramienta que viene a privatizar la censura en un entorno en el que el proveedor de servicios se preocupará más por librarse de responsabilidad que por garantizar los derechos de los usuarios, especialmente en los países en los que no existe tradición reivindicativa por parte de los consumidores. En el ámbito educativo el sistema de notificación del ilícito e identificación de los usuarios, deberá cumplir además con los dispuesto por la *Family Education Rights and Privacy Act*, 20 U.S.C. 1232(g)(b)(2)(B). *Vid.* NACUA, «Copyright peer-to-peer file sharing and DMCA Subpoenas», NACUANOTES, de 6 de noviembre 2003, vol. 2, núm. 1.

[80] Las consecuencias de la retirada material lícito han sido puestos de manifiesto por R. BARCELÓ, R. en «La responsabilidad civil de por daños causados a través de Internet», *en Derecho sobre Internet*, capítulo 12, pág. 19. VVAA, Banco Santander Central Hispano, Madrid, 2000.

tendrán la naturaleza de acto administrativo, por lo que deberán ser dictados en el marco de un procedimiento efectuado a tal efecto, y, en consecuencia, cumplir con el trámite de audiencia a los interesados, sin perjuicio de la adopción de medidas provisionales [81]. Ni que decir tiene que este tipo de medidas (cuanto afecten a contenidos lícitos) pueden llegar a constituir un ejercicio de censura proscrito por el ordenamiento con especial rotundidad cuando proviene de los poderes públicos. Sin embargo en el marco normativo en el que las universidades prestan servicios de intermediación, probablemente las acciones presuntamente ilícitas de los usuarios proporcionen al centro un margen suficiente para iniciar un procedimiento interno o decretar la suspensión del servicios de conformidad con las normas de uso [82] sin entrar a valorar suficientemente la ilicitud de los contenidos alojados.

Se plantea una última cuestión referida a los requerimientos del presunto perjudicado respecto de la identidad del infractor. En la actividad de alojamiento, los datos de identificación no están amparados por el secreto de las comunicaciones sino por el derecho a la intimidad o por la LOPDCP, que, a diferencia de la *Data Protection Act británica* [83], no permite la comunicación de datos a

[81] Las universidades de Granada, el País Vasco, León y Valencia entre otras, han establecido un procedimiento de suspensión del servicio (referido en general a todas las actividades de intermediación) en el que se delimitan las autoridades competentes para acordar la suspensión provisional y definitiva del servicio con la preceptiva audiencia del interesado. No se hace referencia alguna a la fuentes de conocimiento que puedan motivar la imposición de las medidas. Es recomendable que las universidades definan en todos sus extremos un sistema de comunicación de ilícitos que determine el modo de actuar del centro ante potenciales notificaciones.

[82] La mera constatación del uso no académico podría justificar, según la mayor parte de las normas existentes, la suspensión del servicio. No es probable que una motivación de este talante llegara a buen puerto, por un lado por aplicación del principio de igualdad de trato y la tolerancia del uso personal, por otro, por el principio de proporcionalidad.

[83] La *Data Protection Act*, en su sección 35.2 dispone que se pueden comunicar los datos si su entrega es necesaria en el marco de un procedimiento legal, aún referido a la interposición futura de una demanda, o, simplemente, para al asesoramiento legal. En «*Totalise plc v the Motley Fool Ltd and Another*», (QBD), 19 de febrero, 2001 se consideró que el demandado, titular de la página web en la que existía un foro de discusiones, había violado el artículo 35 de la *Data Protection Act*, al negarse a proporcionar información sobre la identidad del usuarios que había incluido mensajes calumniosos en el foro. Motley, al recibir la notificación había retirado de manera inmediata el contenido de los mensajes, pero no proporcionar los datos que pudieran ayudar a dilucidar la identidad del autor de los mensajes, constituía el único obstáculo para interponer la demanda de responsabilidad extracontractual. En EE.UU para obtener del intermediario la identificación del supuesto infractor, el titular de los derechos de autor ha de dirigirse al Tribunal con el fin de que dicte una citación a tal efecto, sección 512 (h) *Copyright Act.*

menos que la solicite algunos de los sujetos a los que se refiere su art. 11, por lo que el centro no está obligado a proporcionar información sobre el destinatario del servicio de alojamiento.

C. *Otras fuentes de responsabilidad relacionadas con la actividad de intermediación*

Al margen de las reglas específicas de los artículos 14 y ss. ha de señalarse que la universidad incurrirá en responsabilidad si incumple los deberes de colaboración que les imponen los artículos 8 y 11 LSSICE. Para el análisis de ambos preceptos me remito a lo expuesto en los restantes artículos de este volumen.